COMMONWEALTH OF AUSTRALIA

Official Committee Hansard

SENATE

LEGAL AND CONSTITUTIONAL REFERENCES COMMITTEE

Reference: Privacy Act 1988

THURSDAY, 19 MAY 2005

SYDNEY

BY AUTHORITY OF THE SENATE

INTERNET

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

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

To search the parliamentary database, go to:
http://parlinfoweb.aph.gov.au

SENATE

LEGAL AND CONSTITUTIONAL REFERENCES COMMITTEE

Thursday, 19 May 2005

Members: Senator Bolkus *(Chair)*, Senator Payne *(Deputy Chair)*, Senators Buckland, Greig, Kirk and Scullion

Substitute members: Senator Mason for Senator Scullion, Senator Stott Despoja for Senator Greig

Participating members: Senators Abetz, Barnett, Bartlett, Mark Bishop, Brandis, Brown, George Campbell, Carr, Chapman, Colbeck, Conroy, Crossin, Eggleston, Chris Evans, Faulkner, Ferguson, Ferris, Harradine, Humphries, Knowles, Lightfoot, Ludwig, Mackay, Mason, McGauran, Murray, Nettle, Robert Ray, Sherry, Stephens, Stott Despoja, Tchen and Watson

Senators in attendance: Senators Bolkus, Buckland, Mason and Stott Despoja

Terms of reference for the inquiry:

To inquire into and report on:

(a) the overall effectiveness and appropriateness of the Privacy Act 1988 as a means by which to protect the privacy of Australians, with particular reference to:

  (i) international comparisons,

  (ii) the capacity of the current legislative regime to respond to new and emerging technologies which have implications for privacy, including:

    (A) 'Smart Card' technology and the potential for this to be used to establish a national identification regime,

    (B) biometric imaging data,

    (C) genetic testing and the potential disclosure and discriminatory use of such information, and

    (D) microchips which can be implanted in human beings (for example, as recently authorised by the United States Food and Drug Administration), and

  (iii) any legislative changes that may help to provide more comprehensive protection or improve the current regime in any way;

(b) the effectiveness of the Privacy Amendment (Private Sector) Act 2000 in extending the privacy scheme to the private sector, and any changes which may enhance its effectiveness; and

(c) the resourcing of the Office of the Federal Privacy Commissioner and whether current levels of funding and the powers available to the Federal Privacy Commissioner enable her to properly fulfil her mandate.

WITNESSES

Committee met at 8.58 am

GRATION, Mr Chris, Consultant, Baycorp Advantage Ltd

STRATTON, Ms Melissa, Group Privacy Adviser, Baycorp Advantage Ltd

WANT, Mr Andrew, Chief Executive Officer, Baycorp Advantage Ltd

CHAIR—I declare open this hearing of the Senate Legal and Constitutional References Committee inquiry into the Privacy Act 1988. This inquiry was referred to the committee by the Senate on 9 December and it is being conducted in accordance with Senate rules and standing orders and in accordance with the terms of reference. We have received over 45 submissions for this inquiry. As I think most people here know, the inquiry's terms of reference require the committee to consider the overall effectiveness and appropriateness of the Privacy Act 1988 as a means by which to protect the privacy of Australians. Witnesses are reminded of the notes they have received relating to parliamentary privilege and the protection of official witnesses. Further copies are available from the secretariat. Witnesses are also reminded that the giving of false or misleading evidence to the committee may constitute a contempt. The committee prefers all evidence to be given in public, but under the Senate's resolutions witnesses do have the right to request to be heard in private session. It is important that witnesses give the committee notice if they intend to do so. I welcome representatives of Baycorp Advantage. Would you like to make any amendments or alterations to your submission or would you prefer to start with an opening statement?

Mr Want—We will leave the submission as it has been presented and we will start straightaway with our statement. Thank you for giving us this time. My colleagues and I are very happy that we are able to speak to the inquiry, which is addressing what we regard as a very important issue—not just for our business, as will become evident as we speak, but also for society at this time. Fundamentally, it seems to us that the question the committee is addressing goes to the future shape of privacy regulation and, in particular, the emerging challenge of finding the right balance between identity freedom and freedom of information.

We are supporters of debate in this space. We believe that the key to the evolution of the regulatory environment now is going to be an open and sustained debate. Baycorp Advantage is keenly interested because essentially our business relies on the finding of this balance. One of the key areas that we are interested in pursuing as part of this debate is the correct approach for the future in relation to data matching. Fundamentally, our business is about creating value through the connection of different pieces of data. In an information economy that is how value is created. Increasingly in the future that is where value will be created. Evidence of that is the efficiency and the benefits that have flown to consumers, business and society in recent years through improved automation of the credit system. Baycorp Advantage has been a key facilitator of that efficient credit provision mechanism that has emerged over the past several years. That has been a driver of the development of the economy and the development of wealth and it has been a strong underpinning of Australia's economic growth. It does create questions of balance.

Without going into detail—we have addressed in our submission areas that we believe are worthy of debate in relation to the act—the act has proved to be a very strong framework for privacy regulation and has stood Australia very well over the last several years. We do think that,

going forward, there will be a need for regulatory reform but, as I have said earlier, we believe that in the lead-up to that what is really needed is a sustained debate about what it is that society wants from the regulatory environment going forward.

Data matching is actually a protection for consumers just as it is a challenge for consumers. The most obvious example of that is identity theft. One of the challenges in the current regime is that there is comparatively little incentive for individuals to take an active interest in the management of their data. Until there is a problem, consumers typically do not look. That comes from a culture which suggests that data which is held about individuals is not their asset; it is something that is held by others to be used against them. It seems to us that one of the challenges is to convert that impression so that people begin to view their personal data as an asset to be managed like any other. In particular, in the information economy that asset will become increasingly important to individuals. So data matching and the mechanisms around data matching are going to be critical for the benefit of consumers just as they are critical for the efficiency of the economy.

The other area in which data matching is clearly going to become a major test for society is the balance between identity management and anonymity in the context of terrorism and security. There is an obvious societal push for greater security following September 11. The risk is that the pendulum might swing too far and individual privacy might be lost in the mix. There needs to be a serious debate about what the benefit for society is and what the policy objective of privacy regulation is in this new context. So it is not just about economic efficiency; it is also about the balance of individual liberty in the face of the challenges society is now dealing with out of the remnants of September 11.

For our part, we want to help encourage that debate—for example, we have invited Baroness Greenfield from the UK to come to Australia in a couple of months time to engage in a seminar and an open forum to talk about exactly these issues. We find it interesting that the UK appears to be adopting a quite centralist approach to privacy management, including looking at options for a single identifier. One of the interesting tests, I think, for us in Australia is going to be whether we want to pursue that sort of route or whether we want to go to some other regime which is far more decentralised—and determining where the relative benefits are for the efficiency of the system on the one hand and privacy of individuals on the other in going down either of those two routes. So we think it is a very interesting debate to be having with the people in the UK who are leading the policy thinking around this area. We are also hoping to be able to bring the UK Information Commissioner to Australia, probably late this year or early next year, to continue that discussion.

In the meantime, while the debate goes on there are things that business can be doing to improve the existing arrangements. In our context, dealing predominantly with credit information at this time, we have set a target of a significant improvement in the operation of the data exchange system around credit information. We have engaged a great deal in recent months with the consumer groups to assess what the concerns of consumer groups are about credit information and the way it is managed today. There are two clear priorities which have emerged from those discussions. The first is that there is a concern that the quality and consistency of data being input into the credit information system is quite poor. There is not a consistent system or framework for the way data is input into the credit information system. For us, that is a significant issue because we hold private data on 14 million Australians—90 per cent of the

adult population and virtually 100 per cent of the credit-active population. We hold similar sorts of data levels in New Zealand.

The integrity of our business and the integrity of our offering to our customers, both consumers and businesses, fundamentally comes down to confidence in the community about the data we hold. For that reason, we have started working with our subscriber base and with consumer groups to improve the framework for data coming into the credit system and to improve the reciprocity of information so that data which is in the system can be relied on by our business customers and, more importantly into the future, can be relied on for accuracy by consumers so that consumers do start to view the information which is held as an asset to be managed.

The second area where we have identified concerns from the consumer representatives is in the lack of a clear path for dispute resolution. Again, this is an area in which we are engaging heavily with our subscriber customers—both to define clear responsibilities within our subscriber organisations for dispute resolutions raised by consumers and to provide an alternative dispute resolution mechanism that consumers can have access to to speed up the process of resolution. We have a very workable relationship—in fact, I think quite a positive relationship—with the Office of the Federal Privacy Commissioner now. I think that has helped significantly to accelerate the resolution of disputes and complaints raised by consumers. In many instances, complaints are now referred directly from the Office of the Federal Privacy Commissioner to us for resolution. I think that has significantly sped up the process for resolution, but there still needs to be a clear path for consumers to pursue where they feel that a data entry in the credit database is not accurate. So they are the two areas that we have identified with the consumer groups as being most key, and we are working very closely with our customer base to improve both those areas.

Moving on to the Office of the Federal Privacy Commissioner: as our submission makes clear, we are supporters of a significant investment in the capabilities of the office and in the resources of the Privacy Commissioner's office. We note that the Privacy Commissioner released a report yesterday which recognises the need for further investment—I suppose that would be regarded as hardly surprising.

Lastly, I should make a comment about the topic of positive reporting—comprehensive credit information reporting—which has been in the press recently. The economic and social case for positive reporting is fairly clear. It is fairly clear that comprehensive reporting improves the quality of credit decisions, improves the efficiency of the credit information system as a whole. Again, there is a very significant difference in the approach taken in the UK by consumer representative organisations in comparison with Australia. In the UK, there is a very strong drive for mandatory comprehensive data provision by institutions into the credit system. The reason for that is that consumer representatives in the UK believe that that will put lending institutions in a position where they can no longer claim not to have the information they need to make a responsible lending decision.

In our view, comprehensive reporting is a win-win situation. It gives consumers the ability to manage their credit history in the most positive way, and that gives them the ability to shop for the best deals and really get the best out of the competitive environment that has been created in consumer lending. For business, there is a clear improvement to the quality of the credit books,

and that is a benefit to the economy. There is a benefit to society generally through improved efficiency in the allocation of credit across the economy. Baycorp Advantage does support the introduction of comprehensive reporting, but we believe that there needs to be agreement with consumer groups that real progress has been made in those two areas I mentioned previously: data quality and reciprocity and access to consumers to clear paths for dispute resolution.

CHAIR—I will ask one question and then we can move around the table. You say in your submission in the context of positive reporting and what is happening at the moment that you get data from a wide variety of sources. What sources do you draw on to compile your data?

Mr Want—The core of our credit information database is provided by our subscriber customers—banks, non-bank lending institutions, telecommunications providers and utilities. An organisation that provides credit in the course of its business will typically provide negative—that is, default—information in relation to lending that it conducts in its business. We are the major custodian of that data.

CHAIR—So it is only negative reporting now?

Mr Want—Correct.

CHAIR—Even from the utilities?

Mr Want—Yes.

CHAIR—And Telstra?

Mr Want—Yes. We are only permitted to hold negative information. We do use other forms of data, as I said before, for matching purposes. We have links with many other organisations—land titles offices; registries of births, deaths and marriages; drivers licence registries et cetera. That information is used to ensure the accuracy of our database for matching purposes.

Senator STOTT DESPOJA—Thank you for your submission. I want to pick up on a point that you made in your opening comments about your relationship with the Privacy Commissioner. You did imply that that relationship was improving, and you said 'now'. When you talk about complaints being 'sped up', to use your term, I wonder whether this marks a change in your dealings with that office or perhaps a change in resource allocation to ensure that these claims have been dealt with more speedily. Or am I reading much too much into your comments?

Mr Want—I think you probably are reading too much into my comments. There is an observation to be made there, and then I will pass over to my colleague Melissa Stratton, who deals with the Privacy Commissioner's office often. I have had most of my dealings with the relatively new Privacy Commissioner. I met her on the day she was appointed or perhaps even before that. I have certainly tried to encourage a very open relationship with the Privacy Commissioner's office, and I can say the same in relation to the New Zealand Privacy Commissioner. In my mind, an open engagement and a genuine dialogue with the Office of the Federal Privacy Commissioner is core to my business. I cannot operate unless I have the community's trust and I cannot operate if I have an antagonistic commissioner, so I need to be

open. We talked about dispute resolution before. There have been some improvements. I cannot actually say, but Melissa can, how recently that change was made. Certainly we have been able to help the Privacy Commissioner's office improve the rate at which disputes are resolved.

Ms Stratton—About 18 months ago the commissioner's office came to us and said they were finding that an increasing number of consumers were coming to them first for dispute resolution—so they had not spoken to us and they had not spoken to their credit provider. Because of the resourcing issues at the commissioner's office they felt that consumers would be best served if they came to us directly—because when we are asked to conduct an investigation we have 30 days in which to complete an investigation. So with the complainants' consent, the commissioner's office will take the complaint, pass it over to us and leave it to us to resolve it with the consumer.

Senator STOTT DESPOJA—Hence the comment about claims being sped up.

Ms Stratton—Yes.

Senator STOTT DESPOJA—In your submission you refer to general support for increased resources for the Privacy Commissioner. I am assuming that, even in spite of some of these improvements, that is still something you support.

Mr Want—Correct. Certainly in the area of complaints resolution there need to be some additional resources. We feel the commissioner's office and the community would benefit from having additional resources to aid in the policy debate—to help explore the areas that we have been discussing about this very sensitive balance that needs to emerge over the next couple of years between freedom of information and freedom of anonymity, if you like.

Senator STOTT DESPOJA—Let me pick up on that, because it sounds like you are certainly doing your bit to encourage debate at various levels. In your submission you refer to consumer rights and consumers being better educated about their rights. Are there any other ideas that you are putting forward, either for government or for the Privacy Commissioner to pursue, in order to ensure that people do have an increased understanding of their consumer or privacy rights in this case?

Mr Want—There are a number. We feel that because, as I said, this is absolutely essential to our business, we have a role to play in education. Fundamentally this is an education exercise. So in addition to promoting debate we are finding ways to help get information to consumers—for example, through a linkage with Yahoo.com.au in Australia and a similar linkage in New Zealand which provides information on credit reporting and how consumers can get access to their own credit information. We are in discussions with the departments of education about trying to build something into the education program. I have had discussions with the financial literacy task force about building a component into that program. So there are various different initiatives we are looking at in addition to simply being more vocal about the topic and encouraging consumers to take an active interest in their credit reports.

Just by way of example: we have something like 200,000 or 220,000 consumers each year coming to Baycorp Advantage asking for copies of their credit reports. That is a tiny fraction of the 14 million credit reports. Ideally we would like to see consumers checking their own credit

reports at least annually just as a matter of good hygiene. How we do that is going to be quite an education challenge, but we have to provide the channels to do it as well. So we have created a system, Mycreditfile.com.au—forgive the plug!—which enables consumers to get online access to their credit report. Then they can check it and come back to us. Clearly the benefit for consumers is that they know their information is accurate. The benefit for us is the same thing: that we know the information is accurate. It is of no benefit to anybody that there should be inaccurate information in the credit system.

Mr Gration—I would like to add to that. One of the other issues that we raised in our submission was the systemic issue around individual consent. That is particularly acute with a data custodian like Baycorp which collects a lot of information indirectly. So consumers can be quite remote from their information. The current regime, part IIIA and the NPPs, relies significantly on individuals to enforce their privacy rights—usually through a consent regime. One of the things we have suggested in our own submission is that, particularly for data custodians, there may be some argument for supplementing that regime of individual rights with some systemic representation of consumer interest, for instance. From the consumers' point of view, their piece of information—their data bit—does not have any much value in and of itself; it only has value as a set. It is a systemic set; the value in it is systemic. So the reliance of the system, in the case of data custodians, on individual consent puts a very heavy reliance on one part of the regime. We see part of the debate that needs to happen as being about supplementing that with some systemic responses.

Senator STOTT DESPOJA—I understand the context within which you are providing that response, but I would like to ask about paragraph 3.4 on page 13 of your submission. You talk about the indirect collection of information but, in particular, you argue or you conclude that the opt-out provision is not changed. In fact, I think your comments are that an opt-in regime would be unnecessarily obstructive of business. That is based on business practice and other experiences that you have had. Can you elaborate on that? In the context of some of those comments, would it not make sense for consumers to have that extra bit of control so that they can opt in as opposed to opting out?

Mr Want—I will talk about the general issue and I will then ask Melissa to respond to the specific. With regard to the consent regime as it stands today, we are not sure what a better answer is but we are not sure that we have the right answer. In theory, while an opt-in regime, or for that matter an opt-out regime, provides consumers with control, the reality is that most consumers do not have any idea, I think, of what consents they have or have not given. A typical person with a car loan, a personal loan, a couple of bank loans and a mobile phone and a gas bill et cetera will have signed dozens and dozens of privacy consents with no way of knowing or remembering what they have signed when. The reality of control is probably a bit illusory. It is better than nothing—there is no question about that. As I said, we do not have the perfect view at this stage, but what we do see is that the current consent regime has some real limitations. Those limitations are going to become much more evident as different types of data are collected and as different pressures emerge for the usage of that data in areas that I mentioned before, such as identity verification for security purposes.

One thing that we believe really does need careful consideration is the secondary use provisions. There needs to be a clear statement of the public interest in data matching for identity verification purposes—of what the public policy objective is. That will then drive the way we

approach issues such as consent and, in particular, it will drive issues around secondary usage. They are general comments.

Mr Gration—I will supplement what Andrew said. There is the 'shine the light' legislation, for instance and a whole lot of legislative initiatives going on in the United States. A lot of them keep focusing on transparency and consent, which requires individual consumers to exercise their rights. We are not arguing to detract from a consent based regime; we do not want to dismantle it. What we are saying is that, in an information society where the volumes of data held keep increasing exponentially, to keep expecting that the regulatory regime will exist solely on a regime of individual consent is insufficient. To go to the question about the opt-in, opt-out, we think there needs to be recognition that there is social and economic value in data matching. We think there does need to be a regime of consent but we think, if there are social concerns expressed as a public interest, we need to find other means of expressing that public interest. For example, in our own case, to move it out of the opt-in, opt-out, we think that there should be systemic representation of the consumer interest on things like data quality and data accuracy so that individual consumers have got their own consent rights but that in the industry forums, for instance, which we are establishing to monitor and benchmark our data quality and accuracy, consumer organisations are represented and can put a view.

Senator MASON—Mr Want, towards the end of your opening statement, you mentioned positive reporting or comprehensive reporting. What is that and what is the difference between that and the current arrangements?

Mr Want—In the current arrangements, the only data that the credit system is allowed to maintain is data about the things people have done wrong. The credit system we have today is very competitive, very fluid and gives consumers the ability to migrate from one credit provider to another, literally in a hour. You go to Harvey Norman and you can buy a new couch. You go to a car yard and you can buy a new car. If you want to switch banks, nowadays it is very easy. State governments have reduced stamp duty on mortgages for the very purpose of encouraging people to shop around. Yet, for a consumer, you cannot prove whether you have managed your credit history well. Under our system, there is no way to know.

Paradoxically, for example, if a consumer makes an application to four different banks for a new mortgage because they want to shop around for the best deal, the way that will show up in our database because of the regime we are operating under is that that is a person hunting around for credit. The credit providers that they are then applying to for credit do not know whether that is a desperate quest to try to find cash flow or whether it is a genuine price based shopping expedition. It does not help the consumer at all. There are many other examples like that.

Senator MASON—You are not just being the consumer's advocate though. Surely there is an interest and an advantage to credit providers here.

Mr Want—There is an advantage to society.

Senator MASON—Society, and credit providers.

Mr Want—I am not suggesting that there would not be benefit for my organisation too. We are not here entirely altruistically. But it is a genuine win-win. It seems to us that the economic

case for comprehensive reporting is very well proven. It is also legitimate to say that Australia's consumer credit regimes have proved very effective up until now. When I talk to our major customers, there is no evidence at the moment of a systemic problem in credit books—notwithstanding the high levels of personal and household debt. The current regime has stood us well. It is a question of what the incremental value is in changing the regime. There is plenty of proof that there is an economic benefit but we believe there is also a consumer benefit. That needs to be discussed.

Senator MASON—In effect it is like positive vetting.

Mr Want—It is a complete view of the consumers' credit behaviours, rather than just the negative.

Senator MASON—Okay; let us take that for a second. You have spoken a lot this morning about privacy and protecting individuals' privacy. Surely that is not the same thing as increasing people's privacy.

Mr Want—No.

Senator MASON—In fact, it is the opposite.

Mr Want—It is the opposite. But it comes back to the question of: is the objective of the system to maintain people's anonymity or to give them more power in the information economy? Are people really benefiting from only having part of their credit history available?

Mr Gration—One of the confusions often made in the debate is between privacy and anonymity. Privacy is the balance between identity and anonymity. Individuals do not have an absolute right in our society to construct their identity as they see fit.

Senator MASON—I accept that.

Mr Gration—For example, if individuals misrepresent their credit history, which is part of their identity, that can often constitute fraud. Part IIIA of the current act sets a balance by restricting the information that can be held to negative information. The question is: is that where we want to set the balance? Privacy is in fact the act of setting that balance between anonymity and identity.

Senator MASON—Hold on. Privacy is not just a word that reflects what you think is the balance. That is not right. The issue here is you want more information to be able to assess people's creditworthiness, and that is fine. But let us not say that that is the same as privacy. I think that is going too far.

Mr Want—Perhaps I can clarify. I think the issue is that we are discussing here privacy regulation, which is about setting that balance.

Senator MASON—Yes, but that is not the same as privacy. You cannot just say we have come up with this balance and that is privacy.

Mr Want—We did not say that.

Senator MASON—You might set it according to the public interest, which is our job, but you cannot say some balance you end up with is privacy.

Mr Want—I do not think we did say that. Just to explore the issue a little further: at a personal level, I think it is important that society allow the right for an individual to be truly anonymous, should they wish to be. If an individual does not want to participate in the benefits of our modern economy and our modern society—they want to sit in a tree in Nimbin or Far North Queensland and have no participation in the system—

Senator MASON—There is no-one like that.

Mr Want—Right. So that is the extreme. Once you move away from that, you are faced with the question of the balance we are discussing to participate in the social security system, in the credit system and in all the other elements of our modern society.

Senator MASON—I accept that.

Mr Want—You are inherently surrendering some of your rights to anonymity. That is really what Chris was saying. It is about where on that continuum we believe the right point of balance is.

Senator BUCKLAND—I have got a couple of questions that I will put on notice because I want to develop them a bit further. There are some questions, however, I want to ask now in the limited time available. I will take up where Senator Stott Despoja left off about the education process. Who should be responsible for educating the public and how much responsibility do you as an organisation have towards that?

Mr Want—I think it needs to be a shared responsibility. I am talking about it as part of general financial literacy. I think it would be wonderful if young people grew up with an understanding of what the credit system is and how they need to manage their own credit, particularly as kids are getting access to credit much earlier nowadays. Mobile phones are the most obvious example of this. Kids can get themselves into a lot of trouble very quickly nowadays at a very young age. So it needs to be shared responsibility, I think, of the lending community and government, which clearly has a role to play in terms of financial literacy and of general education. Whether that is state or federal I think is for others to consider. We believe we have a responsibility. Again, it is not entirely altruistic: it is good for our business for people to participate in the credit information system. The more we encourage that participation, the better the quality of the information we can hold.

Senator BUCKLAND—I have a son in year 10 at school who has just done a project on credit and on privacy; that is, how the information gets passed between one organisation and another. He found it very difficult, even though he is pretty good with the internet, to get very much information at all out of it. He actually went to the bank manager we have known for years and got some help from that. But I did not think there was much available for him to pick up.

Mr Want—In terms of education material? I do not think there is.

Senator BUCKLAND—No. I am wondering whether it should be going down there. As you said, mobile phones can be an absolute disaster for young people.

Mr Want—It needs to be improved. I am not suggesting that we are perfect by any means yet but that is certainly an area we are focusing on.

Senator BUCKLAND—That has answered my question. I appreciate that. The other thing is the method by which information gets passed on. I rely on personal experience in this. I no longer have a credit card and, since I have stopped using a credit card and closed the account, I notice that I do not get letters from financial institutions anymore saying, 'We can offer you this much money. The sky is the limit.' I find that offensive because it means that all my data in the past has been going around to every financial institution in Australia. I used to get regular letters offering me money. That concerns me.

Mr Want—You are raising a very interesting area, this whole area of data driven marketing. Your personal information would not have been shared by one institution with another. In fact, that would be contrary to their competitive interests. What does happen, though, is that a combination of various types of data that relate to you: the fact that you are a public figure and that suggests a certain earnings capability, where you live, the type of car you drive—all these things exist either actually or can be discerned from various different types of data. So there is the capability to have a picture of you as part of a demographic. You probably received that marketing communication as part of a demographic rather than as a particular individual.

Senator BUCKLAND—I appreciate that what you are saying should be right. The difficulty I have with your answer is that I still have the same income level, I still drive the same car, I still live at the same address and I still have the same job, but I am no longer getting flyers telling me how much money I can have. That concerns me greatly. It never bothered me until I closed the account and found that those letters did not come anymore. I do not want the damn things, I have to tell you, but it is offensive that people are having that information.

CHAIR—You could get some now.

Senator BUCKLAND—I just make that comment, and I understand what you are saying in the response. I will ask you the final question now. As I say, I have got other questions that I need to develop a little bit more, from your opening statement. On data matching for security, I agree with you; we need that—but how far do we actually take that? Why do we need to know if I am a Christian, a Muslim, a Buddhist or whatever? Is that a necessary part of security?

Mr Want—I think that is the most challenging question in society today and, to be honest, it is the reason why I took this job—because I find this absolutely fascinating. I think it is going to be a really major challenge for society to find the right balance. One of the scarier issues, for example, beyond biometric data—iris scans and fingerprints—is DNA sampling. Where does this end? The reality is this data exists today. Your DNA and my DNA exist in databases today, so we do not have the option of saying, 'It's bad; let's destroy that data.' That option has gone. We have to as a society turn our minds to how we are going to address this issue. Coming back to the core of the discussion, while the act has been a very strong regime up until now, I think we have to face the fact that, not only in the sheer volume of data being created today but also in the character of the different types of data that are being created today and the different ways that

data can be blended, we are facing a very different challenge now. So there needs to be a lot of discussion about where the balance you are asking about sits.

CHAIR—Has your system been hacked in recent times?

Mr Want—We have extensive security arrangements in place. We monitor that really very actively.

CHAIR—Has it been hacked into?

Mr Want—No system is ever going to be absolutely 100 per cent secure.

CHAIR—Do you keep records of how many times it happens?

Mr Want—Yes, we do. We keep detailed records.

CHAIR—So, over three years, how many times?

Mr Want—I could not answer that question here.

CHAIR—Do you want to take it on notice?

Mr Want—I will take the question on notice, yes.

CHAIR—Thanks very much. Thanks for your submission.

[9.37 am]

JOHNSTON, Ms Anna, Chair, Australian Privacy Foundation

VAILE, Mr David, Vice Chair, Australian Privacy Foundation

CHAIR—Welcome. You have lodged a submission which we have numbered 32. Do you have any alterations or amendments, or would you like to start off with an opening statement?

Ms Johnston—I would like to start with an opening statement. Good morning, Senators. The Australian Privacy Foundation is the leading non-government organisation dedicated to protecting the privacy rights of Australians. Like the Privacy Act itself, we were born out of an extraordinary public outcry over the Australia Card proposal almost 20 years ago. We therefore welcome this review and indeed any opportunity in which Australians can debate, in a comprehensive and informed way, the appropriate balance between the protection of privacy and that of competing interests. Our written submission on this review of the Privacy Act is extensive. I should acknowledge the work of our policy officer, Nigel Waters, in preparing that submission and proffer his apologies to you today for not being here. My colleague David and I will nonetheless endeavour to answer any questions you might have as best we can. However, first I would like to use this brief opening statement to raise some key issues for your consideration. The primary aspect of your terms of reference is:

… the overall effectiveness and appropriateness of the *Privacy Act* … as a means by which to protect the privacy of Australians …

Our submission is that the Privacy Act alone and in its current state is not enough to protect the privacy of Australians. As I said, the Privacy Act is almost 20 years old and deserving of review to ensure its robustness and appropriateness to meet new challenges.

Speaking in very broad terms, we see three main developments in the past 20 years which the act alone cannot affect. The first is the extent to which the so-called war on terror is used to justify an abandonment of any rationality in our policy process, such that new proposals are not calmly weighed in terms of necessity, proportionality or reasonableness, effectiveness and looking at alternative options. The second is the rapid pace of technological change and the third is the use of the Privacy Act as a shield and in some cases as a sword.

I would like to very briefly address the first and last of those three developments. First, on this so-called aged of terror: we reject the notion that we are somehow living in a new age of terror, justifying the abandonment of long-cherished values or hard-won liberties. Commentators better versed in history than I am have drawn sensible parallels with the fear of communism in the 1950s and the Cold War nuclear threats up to the early 1990s.

Senator MASON—Are you saying the threat of communism was not legitimate?

Ms Johnston—No, I am talking about the notion that we are newly in an age of terror and there has never been terrorism or threats before. Our point is that, post September 11, we do not

believe the world actually changed that much. Even more so, we utterly reject any suggestion that privacy or indeed other human rights somehow stand in the way of security or good government. Privacy ensures the freedom of speech and freedom of association necessary for stable and democratic government. Furthermore, privacy, like openness, transparency and freedom of information, is about ensuring the accountability of government and business. In doing so, respect for privacy and the robust enforcement of privacy principles and privacy rights can only strengthen the fair and expose the corrupt.

The third of those issues was the use of the Privacy Act as a shield and as a sword. Our written submission in particular seeks to refute a number of examples in which the phrase 'because of the Privacy Act' has been used inaccurately by organisations, both government and business, as an excuse, usually for not doing something. That practice is frustrating enough for us as privacy advocates as it brings privacy protection into disrepute; however, an even more disturbing development has been the extent to which privacy-invasive proposals are justified or softened in the public's eye through the mere existence of a Privacy Act. That is, the Privacy Act has been used as a shield behind which all sorts of intrusive practices are conveniently sheltered with a bland reassurance along the lines of: 'You can trust us because we are obligated to comply with the Privacy Act.' In this sense, a Privacy Act which is weak, either in its framework or in its enforcement can actually do harm as its mere existence can be used to shut down or sideline public debate or criticism.

A current example is the proposal to radically alter both the nature of the census and the role of the Australian Bureau of Statistics in handling personal data about every Australian. In case you are not aware of that proposal, it is for the ABS to replace the anonymous snapshot of the five-yearly census with instead a permanent movie of every Australian's life. That is the language of the ABS itself—to replace the snapshot with a movie. The result will be a centralised, national population database holding the most extensive collection of data on every person, in an identifiable form. Everything from date of birth, sex, religion and occupation to people's history of disease, their immigration movements and their family relationships will, for the first time, be held in the one place by the Australian government. The Australian Privacy Foundation and, no doubt, other civil liberties groups will be campaigning vigorously against that proposal. However, we do note that the ABS in its discussion paper on this proposal has sought to reassure the public by sheltering behind the mere existence of a Privacy Act.

This new census proposal is the closest thing yet that we have seen to the old Australia Card scheme. Although not featuring a piece of plastic for your wallet, the centralised population database that underpins such a scheme is there, with the proposal to collect richer and deeper data on every Australian than Neal Blewett could have dreamt of in 1987. We know that the Privacy Act alone in its current state can do nothing to prevent that proposal nor can the act alone stand in the way of the inevitable bears being attracted to the honey pot that a national population database presents. Legislation alone cannot protect Australians' privacy. We need informed public debate and absolute political commitment if we are to avoid becoming a surveillance society.

CHAIR—Thank you very much. In your submission you raised concerns that the Privacy Act does not meet international best practice standards. You have also got concerns about the definition of personal information. Could you elaborate on both those issues?

Ms Johnston—I will firstly address the second issue about the definition of personal information. One of the issues addressed in our submission is that the definition in the federal Privacy Act only incorporates information that has been recorded. There is some ambiguity around whether photographs and images are included. By contrast, the New South Wales privacy legislation, for example, quite clearly includes information that has not yet been recorded in a material form. To give an example, the use of live CCTV, where it is not recorded but someone is using surveillance in a live format, is clearly covered by state legislation but not by the federal legislation. Under the federal Privacy Act, there is no coverage for deceased persons. Again, state law covers the privacy rights of people up to 30 years after their death. So there are two examples where the national privacy law is not as strong as New South Wales law, for example.

CHAIR—And the first question, about the international comparisons?

Ms Johnston—One issue is the extent of the coverage of the private sector. That has been the subject of ongoing debate, if you like, between the Australian government and the EU as to whether or not it meets the standards expected by the EU necessary for trade. As we have mentioned in the submission, there is also a project going on at the moment between the APEC economies to develop international standards for those countries. One of the Privacy Foundation's concerns about that is that one of the descriptions of the privacy principles is that it is a privacy-light regime and that the principles are heading for a lowest common denominator rather than a highest common denominator between those economies.

Mr Vaile—I will provide another example. It has come to be recognised that the right to anonymity is a legitimate part of the privacy spectrum and that has been recognised in parts of legislation in Australia, I believe—the NPPs. That does not exist in IPPs in the federal act. This is significant in two ways. Firstly, it relates to the hope to have a provision that explicitly protects the right to anonymity in appropriate circumstances. Secondly, and probably more importantly, in the environment where you have threats to privacy coming in from all directions and everybody and their dog is managing to dream up new reasons to cast it aside, to find loopholes or to weaken protections, having a commitment to the right to anonymity is a shining beacon of privacy, if you like. It is a way of saying that the basic idea that you should be able to be left alone if there is no good reason why not is a very good starting point, rather than the starting point of the data matchers, the surveillance industry and all of those who make money out of compiling dossiers, who say, 'If you have nothing to hide, why are you worried about this?' On both those grounds, I would suggest that the lack of commitment and recognition of anonymity and pseudonymity is something that should be addressed.

Pseudonymity relates to when you are conducting telephone counselling services, for instance, and you have somebody who says: 'This is John. I don't want to tell you who I am. I can't talk anymore now. I will call back tomorrow.' Tomorrow they can still be called John. That is a pseudonym and it is the basis for various sorts of professional communications in various sorts of sensitive crisis environments. It is a counterpart to, or a different version of, anonymity, if you like. I think we would promote both of those things as emerging international best practice which the information privacy principles in the current Privacy Act do not explicitly or implicitly support.

CHAIR—The other issue I have is that you suggest that the national privacy principles should be amended in their application to direct marketing and you suggest the Spam Act model. Can you elaborate on why you think that is appropriate and what sort of mischief that would redress?

Ms Johnston—The Spam Act model is explicitly an opt-in or consent based model. That was obviously developed more recently than the national privacy principles in the broader application to direct marketing. My understanding is that, as a result of the development of the Spam Act project, in which the direct marketing industry was behind the opt-in approach, and as a result of that being seen as a successful model, the Australian direct marketing industry is starting to move towards consideration of opt-in for all direct marketing, in contrast with their counterparts in the US, for example. In that respect, we note that the previous submission, by Baycorp, seems to be a little bit out on a limb in suggesting that opt-out should remain.

To give one recent example: my understanding is that the first successful prosecution in Australia under the Spam Act recently was a company that ran car classifieds or some car sales business. They pleaded guilty under the Spam Act for using SMS to contact customers in other classifieds, such as in major newspapers. They copped their breach of the Spam Act on the chin but they made the point that their competitors could nonetheless call their customers using the telephone and not be subject to the same rules. Partly, in business terms it is about a level playing field between the means of technology. Obviously, the bigger players can afford telephone calls and the smaller players look to rely on email and SMS. They were not actually calling for the Spam Act to be changed but for the playing field to be level so that everyone is working on an opt-in basis.

Mr Vaile—I would like to add a bit of historical context. The Spam Act came in in Australia in 2003, at a time when around the world there was very vigorous interest in spam and the problem of uncontrolled junk communication.

CHAIR—There still is!

Mr Vaile—One of the reasons it still is can be traced back to the resolution of that in the US, the source of probably more than 50 per cent of the world's spam. There was a very vigorous debate. A Californian law and laws in some other states adopted the opt-in principle, which the Australian Spam Act supported, and in fact went further and provided a private right of action if you were the victim of spamming. Unfortunately, in the US as opposed to Australia, the Direct Marketing Association did not accept the business good sense of the opt-in principle and people's right to not have to justify why they did not want to be on a list. At the federal US level the CAN-SPAM Act effectively endorses the opt-out model and is more or less silent about the principle of whether you can send an unsolicited commercial communication.

Consequently, in Australia the level of Australian generated spam, according to my understanding, is reduced quite substantially but in the US, because the federal CAN-SPAM Act overrode the much more stringent opt-in Californian act, you have effectively got a situation where there is no real regulation of spam. Hiding your identity is an offence, and there have been some prosecutions based on that, but it is essentially open slather. As you said, we still have spam with us. There is not much spam coming out of Australia now. I think that demonstrates the effectiveness of the opt-in model versus the opt-out model in terms of suppressing unsolicited

communications, but secondly it also illustrates the difference in business practices and the business environment in America and in Australia.

In my day job at the University of New South Wales we had representatives from the Australian Direct Marketing Association on several forums and symposia that we held. I was actually very surprised to find that they supported the opt-in model. I do not want to put words into their mouths and you would probably be better to take direct evidence on that, but my impression was that they had basically decided that it was better business not to annoy your customers and not to waste money and effort in dealing with unsolicited material. We are hopeful that, because of that rational and enlightened approach, that is likely to be the basis for a broader use of the opt-in principle.

Senator MASON—Can I congratulate you both on your submission—in particular on your reflections on the war on terror. While I do not agree with all of your submission, I think it is both courageous and interesting that you have raised those issues, particularly in the current political debate in Australia or indeed the Western world—so well done.

Ms Johnston—Thank you.

Senator MASON—We are nearly out of time, so I will not ask a substantive question. I want to ask a philosophical question, if that is all right. In the evidence we have been taking over the last few days, privacy advocates always posit the individual versus the state. That is the fundamental divide. I am just wondering whether that is an artificial divide. In liberal philosophy there was always the idea of negative rights: rights against the state. As John Stuart Mill would say, you had to have the right of association, rights to freedom, rights to trial, rights to freedom of speech and so forth, which are rights against the state. But in more recent times there have been positive rights: rights to education, social welfare, security and so forth. With those positive rights surely you have to give away privacy. In other words, with the growth of social welfare and social democratic countries, the idea of a right to privacy is not only impractical but also less justifiable. What do you say to that?

Ms Johnston—We have never claimed that the right to privacy is an absolute right. We understand that it has to be balanced against other rights and other interests. Obviously our concern is to ensure that any proposal or project or whatever is justifiable, that the least privacy-invasive option is taken and that that option is always going to be effective. But certainly we do not necessarily see that privacy automatically stands opposed to or in the way of the pursuit of other rights or other interests.

Senator MASON—That actually is a dichotomy, Ms Johnston. So often you see privacy advocates say that it is 'us representing the individual versus the state'. I think that is a very loose dichotomy when you relate it to a modern society—with the amount of social welfare and with the government being involved in so many areas of our lives. With the war on terror, for example, the greatest threat to privacy can be being molested, and you need some laws about security and law enforcement to protect people from molestation. So the state might be doing something to protect individuals from molestation which surely is, in a sense, an aspect of a right to privacy. I just do not find the dichotomy convincing that so many privacy advocates put before us—because they do.

CHAIR—You may be putting words into her mouth. I am not sure—

Ms Johnston—I am not sure we are necessarily—

Senator MASON—I just want to put it on the record, because it is becoming a bit infuriating that people come before us and say, 'Oh, I am speaking on behalf of the individual versus the government or the state.'

Ms Johnston—On this point I suggest we are in agreement. As I said, we do not see privacy as standing in some absolutely opposed relationship to security or law enforcement. On many issues—as you said, the right to your physical privacy, to be free from assault, and issues such as identity theft and identity fraud—privacy advocates speak as one, I believe, with the law enforcement authorities. The theft of your identity can be an extraordinarily gross violation of your privacy, and therefore we would like to see anything that can handle identity management issues in a responsible way—

Senator MASON—Like an Australia Card?

Ms Johnston—The issue is that we do not believe an Australia Card or any centralised identity management model is the appropriate way to go. We actually think that would increase the risks rather than address them. To use the honey pot argument: the more you centralise the information the more it attracts people; it becomes more valuable for organised criminals or terrorists to hack into the database. When you centralise it they only have to hack into one database or bribe one clerk to get access to the information.

Senator MASON—The British, I think, are going down that path at this very moment, and people like John Stone, who, you would recall, opposed the Australia Card in 1987, are now for it. There is a change of climate, Ms Johnston.

CHAIR—A change of attitude from John Stone—

Senator MASON—He is not a friend of yours—

CHAIR—He has always been known for changing positions.

Ms Johnston—The political climate has certainly changed. What we are suggesting is that the underlying interests have not changed and that there needs to be far more careful consideration of any identity management proposal. In Britain, for example, the London School of Economics has come out with an extraordinarily comprehensive explanation, from a range of fields, as to why a national identity card will make things worse, not better.

Senator MASON—But the House of Lords were not against it.

Ms Johnston—I cannot address that comment.

Mr Vaile—I have a comment on the basic principle. You have raised the emergence of these more positive rights compared to the more traditional base of rights protecting the individual. I think it is worth pointing out that those positive rights effectively in many cases are just treated

as claims which can be advanced or eroded, depending on the flavour of the politics of the day or the particular economic circumstances of whichever country you are in. I would put a more traditionalist case for those liberties which have been fought for over hundreds of years—

Senator MASON—The negative rights.

Mr Vaile—The negative rights being more fundamental and more important for the long-term protection because they are not so reliant on the economics of the day to support them.

Senator MASON—You sound like a liberal, Mr Vaile. It is very liberal of you.

Senator STOTT DESPOJA—A small 'l' liberal—we do not mind those!

Mr Vaile—I am agnostic on these questions, but I would speak in defence of the difference between those traditional protections against the overweening state, if you like, and also the capacity of business, not because of any particular allergy to state or business activities but mostly because of the imbalance of power between those three sectors. There has traditionally been a sort of political imbalance, if you like, between the two in terms of the legal powers available to the state and, to a lesser extent, business. What we are finding now is that those differences are magnified by technology so the individual is still—apart from a few fortunate individuals with great technical resources and education—more or less in the state they always were, but both government and business are now in charge of an increasingly sophisticated and immersive capacity for surveillance and decision making based on what we would consider a wish list, a shopping list, a 'We would love to know everything' approach. For centuries, ordinary life has been able to continue without that sort of incredibly dense surveillance. We would make a case that it is still appropriate to stand back a bit from the flurry of the day and the latest moral panic and say, 'What should we be trying to protect?' At the core, that is some of those traditional liberties.

Senator STOTT DESPOJA—I think I am going to run out of time, so I may have to frame some of my questions on notice, even though I could ask you questions all day. Can I invite you either now or at a later stage to respond to the Privacy Commissioner's review that, you would be aware, was released yesterday. As you know, it is a fairly large review, so not all of us have been able to read it in the detail that it warrants for today. I note that the news release accompanying that review, released by the Attorney-General, stated:

Privacy Review finds legislation working well.

Do you want to respond to whether or not it is working well here today or do you want to take that on notice?

Ms Johnston—I suggest that we will need to take the detail on notice. I have read nothing more than the Privacy Commissioner's media release at this stage. Having said that, our submission both to the Privacy Commissioner's own review and your review, I suggest demonstrates exactly why it is not working. We are not going to say it is a complete disaster but nor do we believe it is adequate. No doubt we will shortly be reviewing Ms Curtis's report and then publishing some kind of response. I would be pleased to make that available to you.

Senator STOTT DESPOJA—Please, if you would. One of the terms of reference of this inquiry, as you know, relates to technological change, in particular to genetic privacy, which is an interest I have. How is your Guthrie card campaign progressing?

Ms Johnston—You are referring to comments I made on the SBS *Insight* program.

Senator STOTT DESPOJA—Yes.

Ms Johnston—Having suggested on that program that I was struggling to find out what was happening in New South Wales in relation to Guthrie cards, I have had further discussions with—I apologise, I cannot remember their names—the various professors who run the newborn screening program at The Children's Hospital at Westmead. They have assured me that in New South Wales they have the practice of destroying Guthrie cards once the person has reached the age of 18 or, on request, earlier but no earlier than two years of age—two years being the period in which they conduct audits of the efficiency of the actual testing. While I was glad to hear that they are destroying it at 18 years of age, nonetheless, that is earlier than the State Records Act suggests for New South Wales, which is 25 years of age.

One of our concerns is that the practices across the states and territories are not uniform, and they are not necessarily clear. I did a Google search on the words 'Guthrie cards' to try and find out about the practices in each state, and none of the New South Wales material came up. That is because apparently Guthrie cards is not the term used anymore—it is 'newborn screening'. Had I searched for newborn screening, I would have come up with the New South Wales material. When I mentioned that to the head of the program at The Children's Hospital at Westmead they suggested that maybe they would need to put the words 'Guthrie cards' back on their web site so that that information came up. That was just a quick test for people trying to find out information. The very fact that the terms can differ from state to state can be an issue.

Senator STOTT DESPOJA—I have to wait 50 years for my son's Guthrie card to be destroyed. Is this a deficiency in the Privacy Act or is this something that requires different or stand-alone legislation or something at a federal level? I am happy for you to answer that in the context of the broader issue of biotechnology, health advances and sensitive health information and not necessarily just specifically in the context of the issue of newborn screening cards.

Ms Johnston—The differences are obviously a product of our federal system of government. One of the issues we have raised in our submission to your inquiry is the need for uniform health privacy standards across the country. Again, we would argue for highest common denominator rather than lowest common denominator or some middle standard. At the moment, all those programs are governed by state and territory laws. Some of the states do not have any privacy laws and there are differences between those that do. I think that is certainly an argument in favour of uniform standards across the country—so long as, in our opinion, they are highest common denominator standards. I think we have mentioned in our submission that we also strongly support in principle the recommendations of the Australian Law Reform Commission on genetic privacy and the need for the establishment of an independent commission to oversee so many of those biotechnological developments.

Senator STOTT DESPOJA—I think the two words you used to describe the political parties exemption were 'hypocritical' and 'unconscionable'. I was hoping you would tell us what you really thought about the political exemption currently under the Privacy Act!

Ms Johnston—I think those two words sum it up.

Senator STOTT DESPOJA—What should we be doing about it?

Ms Johnston—We suggest that you abolish that exemption. Increasingly we believe that political parties operate as large corporations. Again it is an issue of having a level playing field. Other large corporations are subject to the Spam Act, subject to the direct marketing provisions and subject to all the privacy principles that political parties are not. We have seen recently a complaint about the allegation that there were direct marketing calls made to silent home telephone numbers. The complaint could not progress very far because ultimately the Privacy Commissioner concluded she had no jurisdiction. That complaint has faltered. I think that is a graphic illustration of where the exemption causes privacy difficulties.

Mr Vaile—I think it would help the role of both the Privacy Act and the Privacy Commissioner for the population of Australia to see that the politicians and the political parties were prepared to support the core principles of the Privacy Act. One of the most ludicrous examples, if I can put it that way, is in the Spam Act. The Spam Act is only directed to commercial messages; it is not about political communication. There is a an explicit exemption there for free speech for political purposes. The exemption for the political parties in the Spam Act is about marketing their products. I can understand why you would not want restraints on political speech, and I would support that. As far as I can see, there was never any question of that—and the question was answered in any case by the special exemption for political speech. Nevertheless having something that says that political parties are able to sell their T-shirts in a way that only charities are—because in this case they also got an exemption—but every other marketer, including community organisations, non-government organisations and individuals, are not able to had no basis in rational policy. It just seemed like a loophole and it only served to weaken it.

Senator STOTT DESPOJA—I will put the rest of my questions on notice, if that is okay.

Senator BUCKLAND—How do you differentiate between privacy in relation to security—and you mentioned earlier on that you did not think that all that much had changed since September 11—and privacy in relation to financial dealings? Can you differentiate when you are dealing with those two distinct things?

Ms Johnston—I am not sure I understand.

Senator BUCKLAND—How much privacy do we have in giving details if we are travelling overseas and how much privacy do we have if we are borrowing money or having financial dealings? Where is the distinct line? If you look at it now, there does not seem to be much difference between the questions you are asked when dealing with each of those things.

Ms Johnston—I would suggest that both areas suffer from the same fundamental difficulty. The law attempts to impose a consent based regime at many stages—the collection of

information, its secondary use and so on. Regarding the extent to which you are free to give consent if you want a home loan or a credit card and all the banks impose the same requirements on you, how much are you really consenting to? If you want to travel overseas you need a passport. DFAT will give you no choice about whether or not that passport includes a biometric, a radio-frequency identity tag and so on. I suggest that whichever sector you are dealing with or whatever sort of transaction you are looking at, one of the key problems will always be to what extent to you are really able to exercise your privacy rights by providing, withdrawing or refusing to give your consent and, if you decide to refuse to give to your consent, whether your only option is to not travel or not get the home loan.

Senator BUCKLAND—How is your organisation funded?

Ms Johnston—It is purely membership based. We receive the occasional donation. It is an entirely volunteer run organisation.

CHAIR—Thank you for a very valuable submission and evidence.

[10.13 am]

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

CHAIR—Welcome. You have lodged a submission, which we have numbered 15. Do you wish to make any amendments or alterations to it before you make an opening statement?

Mr Britton—Not at this stage. Thank you very much for the opportunity to appear before this committee. In our view, what we are having is a conversation about a gap between what is happening with technology and in the marketplace, and the regulatory and legislative context that is happening in. That is a theme we explored in our submission—that both government and industry have had to act outside the framework to the Privacy Act in areas like spam and there are gaps opening up in areas like surveillance, biometrics and radiofrequency identification. In our view, they are going to need to go on doing so, particularly in the burgeoning field of electronic health records. We are seeing a rapid rollout of electronic health records but little attempt to build a consumer consensus about how these things should be managed, privacy being an integral part of it.

I would like to make some specific comments about a recent case that brings up the question of the deidentification of health data and the backdoor access to electronic health records of consumers. That was the subject of a recent Privacy Commissioner investigation into CAMM Pacific and the Health Communication Network. In that instance CAMM Pacific was receiving information from the Health Communication Network, who were receiving it from doctors running medical director software that was being shipped out to them. That extraction tool was removing information from the medical director software. and it was alleged that it was doing so for all doctors working in group practices, even those who had not elected to participate in the extraction exercise.

On the allegation of this extraction from non-consenting and non-participating doctors, the Privacy Commissioner found that they were satisfied that, if the information were accidentally transferred from a non-consenting doctor, the HCN could not identify the doctor and would not use the deidentified patient data, and found there was no breach. On the broader issue, they found that the patient information transferred was deidentified and, therefore, did not fall into the definition of personal information outlined in the act. On the former issue of non-consenting doctors' patient information, we continue to have an issue with the fact that that data was accessed by somebody, by an agent, in an identified form in order to deidentify it. There was no consent in that circumstance. Somebody was operating the software and, in our view, they were breaching the act and accessing identified health information without permission or consent. It is also material, in our view, to consider that the act is concerned with the collection of information and not the use of it. So we think that the finding that it was not used is not necessarily material to the fact that it was collected under those circumstances.

It also leads us to the broader question of deidentification. In our view, the question of deidentification of data needs to be re-examined and examined carefully. In recent research from the Federal Privacy Commissioner, two-thirds of the 1,500 people surveyed said that a person's

permission should be sought before deidentified data about them was used for research purposes. So there is a considerable sense of ownership by consumers, even if the information has been deidentified. Deidentification is not really well-defined. Is it simply a full medical record with the name and address taken off or is it aggregate data? Our view is that there is certainly a possibility for data to be aggregated to the point where it cannot be reidentified, even if you supply a significant amount of surrounding information to it. In that sense, we acknowledge that data can be deidentified. On the other hand, if data is simply stripped of some identifiers and left otherwise intact, we are not convinced that is in any way deidentified in the sense that it cannot be reidentified.

In the instance of the HCN case, it was possible to link individual patient visits to the doctor in the context of that data stream. So it was identifiable in the sense that you could track back through the data that was provided and possibly build a profile of who that was. A number of solutions have been conjured with—things like statistical techniques or a statistical disclosure control to assess the risk of a deidentification. We think that would probably be pretty intrusive and technical to mandate. There is a notion of using ethics committees to examine research. But the really important thing about ethics committees is that they only give permission where it is infeasible to obtain people's consent and if it is in the public interest. It is important to recognise that the HCN style collection was not for the good of the patients and it was not necessarily for the public good, it was for the profit of drug companies. Secondly, the issue of being infeasible is not just about being a bit costly or somewhat inconvenient. In our view, the best thing to do is to get people's consent.

That is a constant theme which is emerging in the management of consumer data. I think it is important to recognise that privacy is not about secrecy; it is about consumers' control, their permission and their ability to manage that data and participate in the management of it. That is a theme that business does seem to be getting. I refer to some ADMA research—they are following me and will doubtless be keen to elaborate on it—which clearly shows that relevance, trust and consumer control are essential. On the other hand, I have to say that there is one point of departure from their research I would like to get to before they do. It is the finding that acceptance varies by age. Their finding is that the older generation is more likely to hold back on participating in communications, less likely to want to communicate and more reluctant to give personal information. The interpretation made in the research is that the future is bright and that there is a generational shift to engage more with direct marketing. I think that is an assumption. This is not longitudinal research; it is a snapshot, not a movie—to refer to the previous submission. While young consumers are said to be happy to part with personal information to get better service, I think it is also possible to observe that older consumers are also more experienced consumers in dealing with commercial representations and how they manifest themselves. So, rather than a generational shift, I suggest an alternative interpretation would be a plain old learning curve, and one which, in the context of e-health, may be a particularly painful one.

I will make some comments too about the question of open-file credit reporting following on from the comments that Baycorp made earlier. We certainly agree with their points about the fact that there is consumer concern about the accuracy of the current databases. We certainly applaud their efforts to get them accurate but think there is a long way to go. There is also the question of a dispute resolution scheme crying out. That goes to some extent to the resourcing of the Federal Privacy Commissioner. But we do point out that a dispute resolution scheme needs to be

independent. Baycorp cannot be, in our view, its own dispute resolution scheme. It can have a dispute resolution scheme, but we need an effective external dispute resolution scheme.

Some other points to raise just briefly in thumbnail terms are, firstly, that we are also concerned about the symmetry of assertions. There is very little testing of the assertion of debt by companies. We talk a lot about questioning people's assertion of identity—another assertion is that this person is in debt. That is not actually in any way subject to verification before it is put on that database. The next point is the question of who can access that database and the size of the debts listed on that database. At the moment debts of $40 can be listed in there and that can ruin somebody's credit rating. There is a lot of noise in the credit reference system and it needs to be tuned back to being about genuinely important financial transactions, in our view.

The third thing about the open file credit reporting is that it is unexplored economic territory. It really needs to be thought about quite carefully. The effect of having open file credit reporting on the credit marketplace is unknown and untested. It intersects with things like fair contracts terms where somebody could have the interest rate on loan A affected by an occurrence in some other part of their personal life in the term of that contract. That would be a significant change in the culture and would have economic effects as well. Those are some comments arising from that evidence. I welcome your questions.

CHAIR—In your submission you mention concern about a range of new emerging technologies and existing technologies, and one of the debates going on is about whether there needs to be technology specific legislation or whether it be technology neutral. Can you share with us some of your views on that particular point?

Mr Britton—The point I made in the submission is that technological neutrality is a very useful policy and legislative and regulatory tool but what it fails to do properly is risk analysis, because risk typically arises from change and change is specific and poses specific challenges. So we need to be technologically specific in the way that we analyse the risk. However, it is useful to turn that back into a technologically neutral expression of how we are going to deal with that. The minute we actually have a technologically specific solution, we are then immediately ambushed by the next technology that comes along. People sometimes confuse technological neutrality with some sort of static thing that then does not change. It is always going to be challenged and the challenges will be specific. I think there is always the temptation to become specific in the response and I think that is a mistake. It is harder work, but we need to work through what those challenges are and then come up with the technologically neutral response. It gives it longer life but does not mean that then there is a new stasis.

CHAIR—Then you talk about the possibility that industries may develop their own industry code specific to a particular situation. If that is to happen, should it be industry codes or what prescription should there be from the legislative level?

Mr Britton—What we are pointing out in the context of the technical codes is the migration of the code framework from, if you like, the industry silo approach to the horizontal technologies. We are looking at the way the demand has been driven. I do not necessarily think that those are a bad thing but I think they are an uncomfortable fit with the current privacy framework the way it is set up, because it is set up as an industry oriented approach. I do not know that there is a solution to that that is easy to do. The other thing is that much of the

challenge within some of the new technology is to do with surveillance and the expanding envelope beyond the personal information, personal data, filing cabinet metaphor, the data protection metaphor. We are changing the technology into a more fast-moving thing that is tracking people in their daily lives but it still relates to personal information. So I think the gap is probably looking at the surveillance aspects of the way privacy is emerging and the commercial applications of surveillance. We need to think about moving that in a technologically neutral way into the Privacy Act.

Senator BUCKLAND—I have one question; it will probably go into two or three but the principal question is on the trade of information. Again, as you might have heard earlier, I have to call on practical things because I do not have a legal brain. I am fairly simple in thought. I have to deal with things that have occurred and that I am aware of. Prior to going into the Senate, I had a position where I had access to a large number of individuals' details—names, addresses, financial capacity and things like that. I was approached by one company who asked me to provide those names and who made it very lucrative for us to do that. Then they said they would offer more money if I was able to differentiate the individuals as to their earning capacity or likely earning capacity. There was a third one, which I think went to whether they were effective in the work force of non-effective. I am not sure of the term they use but it was if they were on compensation or had a long-term injury or sickness that was keeping them from actually participating in work. My response was to refer the matter to a solicitor and I understand it was dealt with. What deterrents should be put in place, in your organisation's view, to prevent that happening? I do know that some people did participate in the scheme. I found it offensive. How do you deal with that?

Mr Britton—We would see that as commercial misbehaviour, if you like. Commercial misbehaviour is not stamped out by laws but that is not to say we do not have the laws. I think what we need are effective systems—perhaps using the Spam Act as a guide to those sorts of penalties that are there for that sort of misbehaviour, which I think is lacking in the current Privacy Act. We do not have, if you like, a stop point of saying, 'You've done the wrong thing and you're going to get this penalty.' We then need to have a process of complaints handling so that if people think the wrong thing is being done, that can be handled, perhaps short of the ultimate penalty, as it were. Then you need industry associations and self-regulatory systems which actually educate people about what the right thing to do is. Ultimately you need a culture, because that is where this thing really works, of literal self-regulation where people do do the right thing because they know it is the right thing to do.

The touchstone for all this is the consent aspect. What does the person whose information I am holding expect me to be doing with it? What is the consent that I have got that governs my use of it? It may be that you would set yourself up as an information broker with the express purpose of trading this information. If people knew that and for some reason were happy to participate then in that sense there would be nothing wrong with it because people were willing participants in that process. I think that is an interesting thought experiment because I cannot imagine how that would happen, but you have to allow for the possibility that people do freely consent. But then you need a regime that says that, if they have not, they can complain about it and they can have something done about it. If the person persists in doing the wrong thing they will get penalised for doing so.

Senator BUCKLAND—In that instance I had no legal obligation not to pass on the name. There was nothing to prevent me doing that.

Mr Britton—It is a deficiency in the current system, in our view, that you should not trade people's personal information if you do not have their consent to do so.

Senator BUCKLAND—Do you think that can be legislated for or that regulations can be put in to control that?

Mr Britton—Absolutely. In fact, I suspect that under the Privacy Act as it currently stands you would find that, if it was not related to the primary purpose, there would be difficulties. The point is that the Privacy Commissioner does not have many powers of intervention. They may have a possibility of investigating, but there would not be, in our view, anything terribly persuasive they could do to stop it happening.

Senator BUCKLAND—My understanding is that it basically went nowhere when I referred it.

Senator STOTT DESPOJA—I will go back to your comments about generally the consent provisions but in particular your comments at the beginning about consent to deidentify, say, personal or health information. Can you talk us through how you would change the act to provide for those kinds of consent provisions? Or are we looking at, in relation to health information, changes to other laws or even stand-alone legislation that might relate to health information that is acquired as a result of new technology—biotechnology or DNA? I hope you understand what I am trying to get at. Are we looking at some simple changes to consent provisions in the act as it stands to allow for deidentification of health information, or are we looking at other options?

Mr Britton—I think the first thing is that we definitely need harmonised health privacy legislation across Australia. We currently have a real patchwork emerging and there are real concerns about gaps between areas, as well as inconsistencies—not to mention the cost aspects—in a field that is racing ahead. You have transitional authorities and whatnot setting it up. It is all ready to go, and we do not have the framework in place; we do not have the legislative circumstances. I think that is very important. In the process of that we need to iron out things like the consent and the deidentification questions.

The current Privacy Act is not insensitive to the question of health data. There is a whole bunch of stuff there. I guess it revolves around things, particularly in the deidentification area, of exactly what deidentification is. That does not have necessarily have to be legislatively defined, but at the same time we are not getting any jurisprudence coming along to define it in court because none of this stuff gets to court. So we are in a bit of limbo as to how we define a word like deidentify, and we do not even have published authoritative findings from the Privacy Commissioner. It is a rarity for them to give something like that. In fact, here they have just said, 'It's deidentified.' It is quite not clear. For example, is something deidentified simply because the name and address has been removed? We think that is inadequate. It is capable of regulatory resolution, perhaps. Perhaps there need to be guidelines or perhaps we do need to get some things into court to get some judicial interpretation of the word.

Senator STOTT DESPOJA—Is that perhaps one example of where you refer to the powers of the Privacy Commissioner being too restricted, or are there other examples that you think we should be aware of apart from those that you have indicated today?

Mr Britton—I think one of the key things there—and this is something that the Privacy Commissioner has mentioned in her report—

Senator STOTT DESPOJA—So you have read it!

Mr Britton—I have read the executive summary. That was all I got emailed to me.

Senator STOTT DESPOJA—We are getting through it.

Mr Britton—Certainly one of the important things is the recommendation for the ability to make binding codes. I think that in part goes to the question of new technologies and suchlike. It is important for the codes not simply to be those of industry associations but to be able to be the Privacy Commissioner's and to be binding codes on people who use the technologies or participate in the industries. I think that is part of closing some of the gaps in the regulatory ladder, if you like, between self-regulation and legislation. In our view, the joining in the area of privacy is a bit rickety. I thought it was interesting in the context of the remarks from Baycorp about privacy and people's information being an asset, which is an interesting characterisation. I guess it is arguable. But the key point is that if you look at assets and you look at the regulatory regime that is put in place with ASIC and prudential regulation and suchlike, it is an awful lot more rigorous and thorough than the privacy regime we have. In other words, if we are going to start characterising people's personal information as an asset then we are going to beef up our regulatory backstops to that quite considerably.

Senator STOTT DESPOJA—I have one final question. I note that in your submission, when you are talking about smart cards generally and specifically about new drivers licences proposals in Queensland, your comment is that the fact that this could lead to a roll-out should not go unremarked upon. You say:

If the wider utilisation inherent in some of the consequences of the Queensland proposal are rolled out on a national scale, then a national identity card framework may well emerge. This should not occur unremarked.

Certainly not unremarked, but what are you actually proposing? Are you talking about national debates or safeguards or a specific role for federal government in relation to managing some of the implications of not only that technology but the broader idea of a national identity card or framework?

Mr Britton—I think the really important context for that is the acknowledgment that we do have a national identity system now. That is the distributed network, if you like, of identity credentials which is balanced. In some ways it is a really good example of a self-regulating system, because nobody runs it and nobody owns it but it works. It has challenges, but that is part of its self-organising nature. Our concern is that, under technology pressures, elements of that framework may become much more powerful than others, and that is where I am talking about 'unremarked'.

What we could find is that our quite serviceable identity framework, which has the virtues that I just talked about, suddenly gets taken over by a passport that is so powerful and so useful that everybody carries it all the time—I will not go where we have been recently in the news on that—or, equally, by a drivers licence that becomes the credential and then that is all anybody ever wants to see and can see. The point of remarking on it is that in the joining up of the states' systems we could have that happen through the back door—although that makes it sound conspiratorial and it is not. But it will occur in the drivers licence space, unremarked by people that are managing privacy and unremarked by people that are concerned about identity, authentication and the like.

Senator MASON—It is incremental, in effect.

Mr Britton—Incremental, yes, but if you look at it through the network economic lens it has a tipping effect. Suddenly you get to the 80 per cent and—bang!—that is it; there are no other sources of identity that are acceptable. The tipping point can be quite extreme and very quick, and technology, particularly network technology, is characterised by that sort of behaviour. So that could catch us unawares, and suddenly we would have a de facto policy outcome that nobody actually budgeted for, in a sense.

Senator MASON—The people from Baycorp—did you hear their evidence?

Mr Britton—Yes.

Senator MASON—They are a credit reference agency, in effect, and one of the principal issues in the private sector with respect to privacy is credit reporting. They mentioned the idea of positive reporting towards the end of their oral submission, but they did not seem too concerned about the privacy implications of that. Are you?

Mr Britton—That was one of the things that I was remarking on earlier, in the sense that privacy, as I was saying, is not about secrecy, it is not about the capacity of people to hide but about the capacity of people to have control over, have trust in and consent to being part of that system. In those terms, putting open-file credit reporting into the current context, where consumers have poor control, where data integrity is not guaranteed and where there is no symmetry to the assertions in that database, people like those who work in video shops and lawn-mowing men could potentially or actually get access to that database by joining Baycorp. We think that is an extraordinarily dangerous environment in which to put a full record of everybody's private financial life.

Senator MASON—You do think it is dangerous?

Mr Britton—Yes, it is dangerous, but it is not dangerous just because it is a privacy threat; it is dangerous because it could accelerate identity theft.

CHAIR—Isn't it dangerous because of the information systems you put it on?

Mr Britton—That is certainly a big element of it.

CHAIR—And it is not useful without having it on that information system, so where is a safe use of it?

Mr Britton—There are arguments from the proponents of it—

CHAIR—I am asking you. I am not asking for their arguments from you.

Mr Britton—What I am saying is that I can see the arguments they are making about the utility of that information in the credit provision industry, but we are not persuaded that it is safe to put it into the sort of environment we have now and we think there is an extraordinarily large challenge in—

CHAIR—You say 'the sort of the environment we have now': can you conceive of any environment that it would be safe to place it in?

Mr Britton—I have difficulty with it, I have to say, because as I said there is a laundry list of things there—

CHAIR—Let's stop beating around the bush, then!

Mr Britton—It is because you are asking me to conceptualise. What I am saying is that there is a long list of things that would need to be met before it was safe to do it. But, if you put on your economist hat, I suspect the economic arguments are that it would be a good thing.

CHAIR—They are all very simple economic arguments but they are not always the whole picture, are they?

Mr Britton—That is entirely one of the issues of being a consumer advocate: we are economically focused; we want consumers to get a good and fair outcome.

Senator MASON—I yield to your candour!

CHAIR—Thanks very much, Mr Britton.

[10.42 am]

SANGSTER, Miss Jodie, Director, Legal and Regulatory Affairs, Australian Direct Marketing Association

CHAIR—Welcome. Your submission has been numbered 38. Do you wish to amend any aspect of it or would you like to start with an opening statement?

Miss Sangster—As background, ADMA have got 500 member companies and we represent both suppliers of direct marketing and users of direct marketing, so anyone who supplies the direct marketing industry and also companies that use direct marketing either to contact their customers or to make new contacts. The point of clarification, I guess, is that direct marketing is not just about unsolicited outbound contacts. It is also about marketing at any touch point, whether it is with someone you do not currently have a relationship with or someone that is your current customer. Direct marketing covers both those fields.

ADMA recently conducted some research into consumers' attitudes towards both direct marketing and privacy. We really wanted to get an insight into what the consumer is thinking with regards to direct marketing and some of the protections that they would like in place—to get a gauge of their understanding around the Privacy Act. I may make reference to that later on.

There are two areas I want to cover today. Firstly, I have a very general comment about the review of the privacy legislation. We made a number of recommendations which I will cover off briefly with you. The first major general comment with regards to the privacy review is that we really do believe there is an awareness issue that needs to be addressed before a privacy review can take place. Our research showed—and I think also the research conducted by the office of the Federal Privacy Commissioner—that there is quite a low awareness around the Privacy Act itself and even less awareness around the rights that a consumer has under the Privacy Act. For example, we asked consumers how comfortable they felt about providing companies their information. About 53 per cent said that they would feel a lot more comfortable if they knew about their privacy rights, and of those people less than 20 per cent knew what their rights were or that there even was any legislation that had rights for them.

Taking that in context, businesses have obviously tried quite hard to implement the privacy legislation. They have made investments to comply. After making these investments, they are finding that consumers do not know what their rights are. I do not think it is really possible to review whether or not an act is working for the consumer to protect the consumer in a privacy capacity if the consumer does not know what their rights are in the first place. I guess what the direct marketing association is saying is that really the first step needs to be about making consumers aware and investing in making sure that consumers are aware of their rights. Once this has happened and consumers do have some sort of an awareness, there may be gaps that are identified. It is at that stage that a privacy review should take place to look at those gaps and how to address them. So to look at making major reforms to the Privacy Act at this stage is probably premature, and there needs to be a step ahead of that. That is a general comment that I wanted to make.

Notwithstanding that we are saying that we do not want major changes to the Privacy Act, we did make a number of recommendations for some amendments that may address some issues that were actually raised by the Privacy Commissioner. The first recommendation that we made is that consumers should really have a right at any time to say to a company, 'I don't want to receive any further direct marketing from you.' Whereas currently they are given an opportunity right at the outset to say, 'I don't want my data used in this way,' I think it is fair to say that if consumers are receiving marketing that they are not finding is relevant to them then they should be able to go back at a later stage and say to that company, 'I don't want to receive this anymore. Can you please stop marketing to me.' Speaking to our member companies, that is already happening. If somebody does come back to them in that way then obviously the company does not want to marketing to them. It is not business efficient to be marketing to people who do not want to hear from you. So that is our first point.

The second recommendation we made was about the source of data. What we have found is that if consumers receive an unsolicited approach from a company then a major concern to them is that they do not know where that company got their data from. We have found that if consumers are told where their data came from, often a lot of their angst around it goes away.

CHAIR—Or increases.

Miss Sangster—What we have suggested is that, where a customer gets an unsolicited contact, the customer should have a right to ask, 'Where did you get my data from?' and the company that has made that contact should take reasonable steps to let the individual know where that data came from. That will allow the consumer then to go to that person and say, 'Can you please not pass my name out anymore.' The only thing I would say about that is that we have recommended that it be introduced as a guideline in the first instance—the reason being that there are fundraisers, charities and small companies that do not have the systems in place at the moment to deal with that immediately. I suggest introducing that over a period of time—so introduce it as a guideline first and then later on, once they have their systems in place, as a legal requirement.

The third area that we made a recommendation with respect to was actually in response to a concern that the Privacy Commissioner raised around indirect collection of data—so collecting data from someone other than the individual themselves where the company is collecting it for the primary purpose of direct marketing. It seems that there is a gap in the legislation there in that if you indirectly collect data for the primary purpose of direct marketing then there is currently no requirement to give that individual an opportunity to opt out of receiving anything further. So we have suggested that, where data is collected not from the individual, in the first marketing approach there should be something expressly in there that says, 'If you don't wish to receive further marketing, please let us know.' It should tell the individual how to do that. That obviously would be backed up by this right for the individual to be able to opt out at any time.

The last recommendation that we made was in regard to making a distinction between a data owner and a data processor. This is quite important in the direct marketing industry because often someone who owns data will outsource to another company to perform operations on that data—to clean it up, to take off the suppressions and that sort of thing. A distinction needs to be made between the two because currently under the Privacy Act the data owner and the data processor are seen as two separate entities. Obviously all of the requirements in regard to the

disclosure and the collection of data do apply between those parties. That is probably something that needs to be addressed.

CHAIR—I want to just raise a question that has been put to us—that is, that the Privacy Act should be brought into line with the Spam Act when it comes to direct marketing. The experience of some of your members may very well be that that might be a useful way to go.

Miss Sangster—That is not a move that our membership supports. We do believe that the Privacy Act is really around the use of data—it is not about regulating channels—and the Spam Act is about regulating the use of a channel. So, for that reason, we do not believe that they should be brought into line with each other. The other point is that with regard to something like direct mail—which is quite different from receiving, say, an SMS message—the level of intrusion is quite different. So a consumer who receives direct mail, providing they are given an opportunity to opt out, is given adequate protection there, whereas it is obvious with something like a text message, which is an awful lot more personal and a lot more intrusive, that further protection is needed.

CHAIR—Is that right, though, when you come home to find that your letterbox is full of direct mail? Isn't that as offensive and as intrusive?

Miss Sangster—I think we have to look at a balance here because, at the same time, if we made it so that it was a consent based or an opt-in approach then consumers would not know about all of the products and services that are available out there for them.

CHAIR—They will know about the ones they want to know about.

Miss Sangster—The problem is that what you will have is that the consumers will know about the big companies with a brand, and the consumers will be able to ask for marketing material from those companies, but the smaller companies that do not have a brand reputation and have not managed to establish themselves will not have that opportunity. So when we are talking about a balance we are saying, 'Let the consumer know, and if the consumer is not interested or does not want to hear from you then there is the way to say, "I don't want to hear from you anymore".' That allows a balance—it allows the consumer to get the information and to be made aware of things but at the same time to say no if they want to.

Senator BUCKLAND—But that is suggesting that Coles, Woolworths or Harvey Norman are not known to anyone.

Miss Sangster—No, I am saying that they are known to people.

Senator BUCKLAND—Well why do they have to direct market in the manner that they do? What you just said was that well-known companies do not need to market, yet they are the ones who fill your letterbox.

Miss Sangster—What I am saying is that there needs to be a balance between the companies that have an established, well-known brand that the consumer will go to and your smaller supplier who has not got that reputation and is not going to put on a level playing field if that is the case.

Senator MASON—You are trying to facilitate commercial activity, in a sense, aren't you?

Miss Sangster—That is what I am saying.

Senator BUCKLAND—That was an intriguing statement, because that is just not right. You did make a couple of points earlier to the effect that it is pointless direct marketing to people who do not want something. Let me assure you that in the last three weeks my wife or I have again contacted four organisations who have contacted us relentlessly since Christmas and each time said that we do not need a follow-up. You say that that is all we need to do. That is a nonsense. What do you suggest we do to actually stop that? What does your association say we should do to stop that?

Miss Sangster—This is the reason we have made a suggestion that an individual should be able to opt out at any time and that there should be a legal requirement for the company to then stop contacting that person. Currently the Privacy Act does not have a provision in it that says that if you go back to a company and say, 'Please stop marketing to me,' the company has to stop that.

Senator BUCKLAND—What is your recommended legal requirement?

Miss Sangster—That in the Privacy Act there be a provision that says that if a consumer requests to receive no further direct marketing from a company then that company ceases to market to that person.

Senator BUCKLAND—And if they continue to do it, what penalty do you recommend?

Miss Sangster—It would be the penalties under the Privacy Act. That is obviously not for me to decide.

Senator BUCKLAND—At the very beginning of your submission you said that you had had a survey carried out. Did you carry that out yourselves?

Miss Sangster—We commissioned the research and we actually conducted it with the University of New South Wales. It was carried out by Taylor Nelson Sofres on our behalf.

Senator BUCKLAND—Can you give us a ballpark figure of what that might have cost?

Miss Sangster—Do you mean the cost of the research?

Senator BUCKLAND—Yes, or is that private?

Miss Sangster—I can give you a ballpark figure of around $150,000.

Senator BUCKLAND—How much does your organisation contribute to the education of consumers regarding direct marketing?

Ms Sangster—We contribute to the education of consumers through our do not contact services.

Senator BUCKLAND—Explain that to me.

Miss Sangster—We have to market our do not contact services. We also have a number of guidelines for consumers. We have a consumer section of our web site that we develop. We have a consumer version of the code of practice.

Senator BUCKLAND—How do I get this information if I have not got the internet?

Miss Sangster—You can phone us, and we will provide you with that information.

Senator BUCKLAND—How often do you advertise, 'Phone us and we'll give you this information'? It is pretty important, isn't it?

Miss Sangster—I also think that we need to bear in mind that our association is representing direct marketers. It is not a consumers association and obviously we are there to represent direct marketers. We will do as much as we can to educate consumers at the same time, but that is not our principal reason for being.

Senator BUCKLAND—As a representative body, I assume there are times when you get together with your members. Do you ever discuss how much you might contribute to education?

Miss Sangster—We do discuss that and we have a councils framework which looks after each direct marketing channel. Initiatives for things like consumer guidelines come from those councils. No, it probably is not discussed in monetary terms but, yes, we do discuss initiatives to make consumers aware of issues surrounding direct marketing.

Senator BUCKLAND—Would you be able to provide the committee with the amount that has been spent over the last three financial years on educating the public?

Miss Sangster—No, I cannot provide that figure to you at this committee hearing.

Senator BUCKLAND—Can you take that on notice?

Miss Sangster—It would be a difficult thing for us to do. If you wanted us to spend time doing that, then it is a possibility that we could do it. It is going into things like the printing of guidelines. If it is necessary for the purpose of the privacy review, we can do that, but I am not sure it is particularly relevant.

CHAIR—Can you see what might be readily available? You raised the point initially about the need for education as a primary step before we address the legislation. I have to say that that is just a way of putting it off, because you could spend the rest of anyone's life educating the next generation of consumers. Some of these legislative issues need to be addressed earlier than at the end of an education process which may be never-ending.

Miss Sangster—I am not sure I strictly agree with that. I think that the government has a very important role to play, if they are going to give consumers rights, that they let consumers know what those rights are. The research has shown from both the Privacy Commission and from our own research that the levels of awareness are extremely low. I do not think it is particularly for

the government to be pushing it back onto industry to be educating consumers, as much as we are willing to be involved in that.

CHAIR—That was not my point, Miss Sangster; the point I was making was that you may need to get the legislation in place to actually provide those rights. You do not leave that process until you have educated everybody in the electorate, because that is almost an impossible thing to do.

Miss Sangster—I think the point I was trying to make is that we do not know at the moment the extent to which the act is working or not working. If consumers are not aware of their rights and they cannot assert them then it is very difficult for us to tell whether consumers are happy with the legislation that they have got.

CHAIR—But what we are saying is that there should be some rules and guidelines governing the industry. We have got to make—

Miss Sangster—There are.

CHAIR—There are, and a lot of the evidence that has come before us indicates that they are not adequate. The experience of, obviously, members of this committee would indicate that they are not adequate because it is not working.

Miss Sangster—But where did the evidence come from that it is not adequate? I am not sure if that is coming from the consumer.

CHAIR—We are getting evidence from you saying that it is adequate. Other people have got the right to come to us and say it is not. If you go and look at the committee's web site you will find lots of submissions indicating that people have concerns about all sorts of aspects of direct marketing or other aspects of privacy. That is where you will find it.

Miss Sangster—But I think an important point is that there is not an awful lot of research being done with consumers to say to consumers, 'What are your concerns?' I think there is an awful lot of representation from consumer bodies possibly, but the actual research—

CHAIR—Sure, but you do not need research to know that someone is driving you mad on the phone ringing you up telling you your football club is such and such and that you are in for an offer because you are a privileged member of that club. You do not need research to know that that is an intrusion of privacy. Senator Mason.

Miss Sangster—Can I respond to that?

CHAIR—Yes.

Senator STOTT DESPOJA—I think the right of response is fair enough.

Miss Sangster—With regard to your example about a consumer who is receiving telephone calls, if a consumer knew their rights with regard to who is meant to have their data and what they could do to stop that, that would help them.

CHAIR—It did not stop it. For a whole weekend the phone calls did not stop coming. And then it came the following week.

Miss Sangster—But that is one example. It can be any industry—you can mention the banking industry and as soon as you say that everyone has a gripe about banking. I think that we have to take it in context. But the general point being made is that if a consumer knows how to handle it they feel a lot more in control of data. We have got evidence to show that through the research that we have done.

Senator MASON—In relation to the European Union, you argue in your submission that the European Union's failure to recognise Australia's Privacy Act has not hindered the ability to conduct business with European counterparts. I think in your submission also you refer to the very broad definition that the Europeans adopt in regard to personal information. Our Privacy Act, as you know, was developed partly from European protocols developed in the 1980s, and the argument has always been that if our privacy protections are not up to scratch, that will hinder our trade with the European Union. What is your response to that?

Miss Sangster—My response is that because Australia's privacy regime has not been recognised by the European Union businesses have had to find other ways of operating. If they are going to operate with companies overseas they have had to find other ways of operating, which have generally come down to contractual arrangements they have established. A majority of companies have actually done that now—we have been in the process now for a couple of years. That is a practice that companies have adopted.

I think the other suggestion I made was that it might be useful to have a standard form contract to actually help those organisations that have not got to that stage and that possibly are not currently transferring data overseas. It would just help them with that process.

Senator MASON—So Australia's weaker privacy laws have not hindered trade with the European Union?

Miss Sangster—I would not say they are weaker privacy laws; I would say they are different privacy laws.

Senator MASON—Oh, I don't know if the committee would agree with that distinction. Would you agree with that, Senator Stott Despoja? I suspect not!

Miss Sangster—I am allowed to say that as I specialised in data protection law. The point I am making is that there was a concern that if we were not recognised by the European Union that European companies would not trade with companies based in Australia, but that has not been the case, because it has been overcome by contractual arrangements.

Senator MASON—Whether that is a good thing or a bad thing is another question.

CHAIR—Thank you very much.

[11.03 am]

ADAMS, Ms Carolyn, Principal Legal Officer, Australian Law Reform Commission

WEISBROT, Professor David, President, Australian Law Reform Commission

CHAIR—Welcome, Professor Weisbrot and Ms Adams. Your submission has been numbered 18. Do you wish to amend or alter it, or would you like to start with an opening statement?

Prof. Weisbrot—There is just one typo which you might have picked up. On page 3, paragraph 8, where the fourth line says, 'there are circumstances in which genetic information may amount', it should say, 'may not amount'. There is a missing 'not' at the end of that sentence. I think the context later makes that obvious anyway, but I was horrified to find that this morning when I re-read the submission. Otherwise the submission stands as it is.

CHAIR—Thank you. Would you like to start with a statement?

Prof. Weisbrot—I will not make too much of one other than to say again that this statement is drawn from the work that the ALRC did in association with the Australian Health Ethics Committee of the NHMRC in our reference on the protection of human genetic information. In that inquiry, we had three bullet points, if you like, that carried through the whole inquiry. One of them was to look at privacy protection, another was to look at issues of unlawful discrimination and the final one was about issues of maintaining the highest possible ethical standards.

We then took that across a very wide array of subject matter, including those in the medical and health area, like clinical research, the deliverance of clinical services, public health administration, genetic databases and so on. On the more medical legal side, we looked at issues of insurance, immigration, employment, the use in sport, the delivery of services and a range of other issues, including identity testing, whether that was done for parentage purposes or the potential—I think harmful potential—in using it to determine race or ethnicity in the case of Aboriginality, and a range of related matters. The privacy concerns, as I said, were looked at in a wide array of contexts.

There is just one update. In paragraph 4, we noted at the time of the submission that the government had not yet formally responded. That is still the case. We understand that there is a whole-of-government response in preparation. I gave the Sir Ronald Wilson annual lecture in Perth a week ago. The *West Australian* contacted the minister's office—Tony Abbott's office—and asked what the state of play was. The quoted material in the *West Australian* was 'soon'. We hope that is certainly the case. I understand that informally.

In terms of direct action, in last Tuesday's budget—although for some reason it was overshadowed by $22 billion in tax cuts!—the government allocated $7.6 million to establish a human genetics advisory committee. That would be another principal committee of the NHMRC. That basically implements the central recommendation of the ALRC's report, which is that we need a standing committee to monitor developments in this area and to provide expert

advice—both technical scientific advice and advice about the ethical, legal and social implications of the new genetics.

CHAIR—I will start off with one question about employee records. You mentioned those on page 7, I think, of your submission. Could you explain what you think the need is and—I think you say federal legislation—why it should be federal legislation?

Prof. Weisbrot—We are reporting to the federal government and looking at the federal Privacy Act in our report so our recommendations were addressed to the federal government and federal parliament, although in many areas we made a template or a parallel recommendation that the states and territories, where they have legislation in place, should act in train. But in this case, as we understood it, the intention was eventually to cover somewhere the privacy aspects of employee records. The government expressed a preference to deal with it in workplace relations. That has not happened yet. Our preference, after studying the area, in any event, would be to give it the same sort of protection that is accorded more generally under the Privacy Act.

Privacy protection is given to personal information, including health information. We thought that this was particularly sensitive in the area of employee records. We have a chapter and many recommendations that relate to employment in the report. Although in one way the primary battleground about genetic discrimination overseas has been in the area of insurance, our prediction was that in Australia it would primarily be in the area of employment. That is because our insurance system is different. We do not use insurance to secure mortgages, for example, as they do in the UK, where they do not, sadly, have Torrens title and therefore operate in a different way. So that has been a major battle there. We do not have the issues they have in the US about the lack of any comprehensive medical system. We have community rated top-up private health insurance so there is no individual risk assessment there. While there are big issues for the insurance industry that we deal with and that they are dealing with, we thought employment was a particularly significant issue here.

At the moment there is really no regulation of the right of an employer to hold that information or to ask for that information. So we made a comprehensive set of recommendations in that area, dealing with employment. Those recommendations were fairly interventionist, saying that we think as a general rule employers should not be asking for or using predictive health information in making decisions about employment.

In order to bolster that, we thought that the Privacy Act had to also reflect that view. Interestingly enough, earlier on the groups that represent employers, particularly the ACCI, said that they did not want any alteration to the existing regime in respect of employment records, but by the end of the inquiry they acknowledged in their submission that they thought this was such a sensitive area that they would accept the amendment of the Privacy Act to cover genetic information at least in relation to employment records.

CHAIR—So you say the Privacy Act should be amended—not the Workplace Relations Act?

Prof. Weisbrot—That is our preference, yes. We have difficulty seeing exactly how you would do that in the Workplace Relations Act. I think you would have to add a whole new division, which would substantially replicate what you already have in the Privacy Act, and it is unclear to us why you would do that, although it is technically possible.

Senator STOTT DESPOJA—First of all—this is my first opportunity to get this on record in this context—congratulations to you and the ALRC and the AHEC for your work on *Essentially yours*. When I asked the Senate and Minister Ellison last week, during the debate on the family law bills, about when we could expect a response to your report, he said, 'Shortly'. So you have 'Soon' and we have 'Shortly'.

Prof. Weisbrot—Is shortly better than soon?

Senator STOTT DESPOJA—Have you no more specific a time line than that? No-one has given you an impression?

Prof. Weisbrot—Only very informally. It is a report that cuts across many portfolios, and I think that is the issue. It is being primarily coordinated by Health, and the Attorney-General's Department has been involved and active. But, looking at the subject matter here, my guess is that you would also have to deal with DIMIA, Workplace Relations, Education, Science and Technology, DFAT and, no doubt, a range of other departments. So I think it is probably a very large coordination project, and involves getting the sign off from all the various ministers and so on. I am not aware that there are any major issues of principle holding things up. I suspect it is more a question of the coordination. But again that is a third-party process impression. I am not directly involved in that process; I am just, as you are, a very interested observer.

Senator STOTT DESPOJA—He did say it was currently with the Standing Committee of Attorneys-General. I was wondering whether you or the ALRC had been invited to speak to that—no doubt august—body.

Prof. Weisbrot—Not directly. They may think we have said quite enough on the subject.

Senator STOTT DESPOJA—Indeed. Just touching on the budget, because you brought up the allocation of $7.6 million over four years to the advisory committee—indeed it was overshadowed by tax cuts, despite the best attempts of some of us to whip into a frenzy the Australian media and community—it does differ somewhat from the recommendations in your report. You came up with a stand-alone, independent statutory authority in the form of a commission. Do you have any ideas as to what this advisory committee, as part of NHMRC, will do or, like us, do you only have the budget papers to refer to in terms of its role and responsibilities?

Prof. Weisbrot—That is all that has been developed. That is all I have seen at the moment. So it will require an amendment to the NHMRC Act because all the principal committees are separately provided for there. I understand the NHMRC Act is being reviewed anyway, so I suspect it will be part of some greater number of amendments. So what we will need to know is exactly what that legislation says and what terms of reference it has.

Although our first preferred model is to have a stand-alone commission, our second preferred model is for it to be a principal committee of the NHMRC—and all the recommendations we made would be equally applicable to that, in terms of what area should be covered. We still think it should be a standards setting and advisory and coordination education body, rather than a regulator, and that the regulation function should go to other bodies that normally have that function.

The concerns we expressed there about why a commission might be the better way to go related to the following: the fact that a commission would be likely to attract adequate resources, although I am reassured by the allocation that has been made now that it will have adequate resources to do the job; and, secondly, that not all the issues were purely health related. Just as the Family Court's obligation is to look after the rights of the child, the NHMRC's overriding obligation is to look after the health of Australians.

There are some issues in here—for example, parentage testing and some others—which you could probably shoehorn in, as you could shoehorn almost everything into the issue of health, but they do not fit as neatly as you would like for normal NHMRC operations. Having said that, they may be able to take on those issues anyway and deal with them adequately. That was the reason we went for the stand-alone. I was reasonably certain that we would get the principal committee and that is because I understood the NHMRC was lobbying to get it and I thought that was the most likely outcome, even though we felt we should still go with our best advice.

Senator STOTT DESPOJA—So you were not consulted about the budget proposals specifically? You were not alerted to that proposal?

Prof. Weisbrot—No, I found out about it more or less on the night before as well.

Senator STOTT DESPOJA—Right. I note that the wording in the budget papers is almost identical to the recommendation in your report—in fact it is pretty much word for word in relation to the perceived responsibilities of the committee.

Prof. Weisbrot—They were taken out of the report but not directly from me.

Senator STOTT DESPOJA—You mentioned the Family Court. You would be aware of aspects of the debate that took place in the Senate last week in relation to parentage testing specifically, as part of amendments relating to the ability of maintenance to be repaid to a father who can prove that a child is not his—whether that is through deception or other means; we do not know how that is established. Surrounding that change to the law, I could not see any particular safeguards or amendments to that legislation to deal with the very complex and vexed issue of parentage testing. Are you aware of the changes that took place last week and do you have any comment for this committee given that parentage testing is part of your work in the ALRC report and also part of your submission in relation to genetic privacy? Do we have adequate safeguards generally and in the Family Law Act specifically that deal with parentage testing?

Prof. Weisbrot—Separate to the process that you were involved in last week, the family law regulations were changed in accordance with the ALRC recommendations relatively recently—and I am sorry that I did not bring that material with me but I can provide that on notice. There was change to upgrade the identification and consent requirements in relation to laboratory testing for parentage purposes and that is what we did recommend in the report. So that has been done separately and did not require legislation; it was a new regulation. That was exactly in the terms that the ALRC recommended. So there are some improvements there.

The other things that we recommended, which have not yet been implemented and may be part of this government response or not, are having only accredited labs doing the testing. At the

moment unaccredited laboratories are allowed to do it and to report a result for parentage testing purposes. We said that only NATA-accredited labs accredited for that purpose should be able to do that and report a result and only those results should have evidentiary weight in any Australian court or tribunal. So that has not yet come in.

We also made a parallel recommendation, which I think runs through some of the other areas in the Privacy Act as well. We felt so strongly about the integrity of the individual to be free from non-consensual testing—and, I should emphasise, not only in the parentage area but across the board, whether it is an insurance company, government, the media or others—that we recommended the implementation and establishment of a new crime of taking someone else's DNA and submitting it for testing without that person's consent or without other lawful authority. The other lawful authority could be an order from the Family Court or another court that orders paternity testing or it could be a statutory authority where a law enforcement officer has to take DNA samples for the purposes of a criminal investigation or it could be research that is being done under a Human Research Ethics Committee approved process. But we felt that surreptitious testing should be sanctioned.

I have spent most of my career arguing against the indiscriminate use of the criminal law and regulation and its increasing intrusion. But this was an area where we felt that, because DNA material is so readily obtainable—we are constantly sloughing off DNA—and it was easier to get a hold of and it was easier to test without someone's consent, particularly by an unaccredited lab which did not have the same ethical standards, we needed that strong sanction to be brought in.

The UK Human Genetics Commission has made a similar recommendation that is in a bill before the UK parliament at the moment. I am not aware of what the progress on that has been. So we are not the first jurisdiction to recommend that. I think we were roughly equal in recommending it but they are the first to move towards action on it. That would have some of the effect that you are talking about here in trying to provide a stronger sanction for unregulated testing.

Senator STOTT DESPOJA—So without the implementation of the six out of seven recommendations that the ALRC has made on parentage testing, is it feasible that people—say, in this case, a father—could obtain a DNA sample from a child without consent, regardless of the age of the child, and take it to a laboratory that is not NATA accredited, and that would be admissible in court?

Prof. Weisbrot—You would make the argument that it was unlawfully obtained evidence, and you would have that. Those courts have discretion at the moment, with the Family Court and the Federal Magistrates Court operating under the uniform Evidence Act. It would drill down to those discretionary provisions in which the court could admit it or not, depending on whether its prejudicial nature overwhelmed its probative value. I would hope the courts would not admit that evidence. I am not aware of any precedent, off the top of my head, but that would be the evidentiary position. We thought that needed to be bolstered by a stronger disincentive and, as I said, that has not yet been determined by government.

Senator STOTT DESPOJA—I do not mean to throw these hypotheticals at you that are so specific, but I am interested in the issue of consent throughout this act and particularly consent in

relation to genetic privacy. Last week threw up a number of cases for us to start considering—preferably before we amended the act accordingly—for example, the case of a 12-year-old child where someone has asked for a strand of their hair, a saliva swab or whatever it might be. I am just wondering how protected they are or what rights they have over their own genetic information and the privacy of that information. I am finding it hard to work out exactly what rights they do have.

Prof. Weisbrot—They are not well protected at the moment in terms of what you might call curiosity testing, leaving aside what legal implications it has, because it is quite easy to get a child's or an adult's genetic material. You can get it from hair, a toothbrush, a buckle swab that you get as part of a game that you are playing, a tiny little blood sample. So it is very easy to get the material. It is very easy to then put it in a little plastic bag and have it tested by a lab either in Australia or overseas and to get a report. The person who does that would then supply their genetic material and it is very easy to do a match to have, say, 99 per cent more confidence in whether the people are biological relatives or not. So there is little protection at the moment. Again, our recommendation said that that should only be pursued on the basis of consent.

In relation to children, parallel to the report we did on the rights of the child some four or five years ago, we said that children should be involved in that decision making if they were sufficiently mature. If they were not and they needed their interests protected, again that is the role of the Family Court or the Federal Magistrates Court. To the extent possible it should be a consensual decision.

The submissions we received from fathers' groups, I note, overwhelmingly said that they should be able to do that without consent, because they had a presumptive right to know whether or not the child is a biological relative. We thought the language of rights in that area was particularly unhelpful because all of the individuals concerned had rights, and we were talking about the intersection of those. If you cannot get consent, that is quintessentially what the courts are there for—to try to balance those rights. We thought that unilateral action was inappropriate in asserting one person's rights there. So we hope for consent. We know that in the real world that does not always happen, particularly in an area of fraught family law relationships, so the courts would act as independent arbiters where that was relevant.

But it is still technically possible and it is getting easier, in the absence of legal regulation, for that genetic testing to occur because the material is so readily obtainable and the costs of genetic testing are going way down. If you do a quick experiment and type 'genetic testing' into Google, you will find it throws up hundreds or thousands of pages of offers of quick, easy and cheap genetic testing—some of them in Australia, most of them overseas—so it is quite doable in terms of practicability. That is why we thought we needed quite strong legal disincentives to prevent illicit testing happening.

When we spoke to men's groups, they were of course focused on this particular area. They were literally being patronising—which I guess may be appropriate in the circumstances. We were saying, 'How would you feel if your employer took the same approach? What if they said, "John's looking a bit peaky. We don't want to alarm him, because probably nothing is wrong, but we will just get a bit of genetic material, whack it in a plastic bag, send it off and get the report back. If it says he's in good health, fine; we won't raise it. But if something's wrong then we'll

take action"'? They were fairly irate about that. If you change the context, people have strong views about the dignity of their body and their autonomy over their own genetic material.

Of course, the advantage of the ALRC working in this big project mode was that we looked across the board. We looked at the same issues that would come up in employment, insurance, immigration, medical research, parentage testing and so on. Our recommendations were consistent across the board—that is, that these things should proceed with informed consent and that, if that was not possible for one reason or another, you needed another formal mechanism like a court order or the ability of the NHMRC to override consent for varied medical research and that sort of thing. But you need that formal mechanism rather than vigilantism to do this properly.

Senator STOTT DESPOJA—I take on board your opening comments about the differences between, say, the American system and our own, particularly in relation to insurance and employment. I understand that is at the heart of your conclusions in the ALRC document and it is indeed why you did not necessarily support, say, stand-alone legislation in the form that I have proposed. Admittedly, my private member's bill was modelled on American law. Mind you, that is getting very old anyway and was always intended to get the debate going. You do conclude in your submission here that the Privacy Act does not currently cover genetic samples, even where these are identifiable to an individual et cetera, and you raise the difficulties in jurisdiction, with the possible exception of New South Wales. You have talked about broad support for the extension of the Privacy Act to cover these areas. Is that a starting point for this committee in terms of our analysis and recommendations? Should we be looking at amendments to the Privacy Act to deal with the protection of genetic information?

Prof. Weisbrot—There were a number of recommendations that we made. One was that it should squarely refer to genetic information. At the moment, it talks about health information or personal information. We thought that it needed a specific reference. That is partly a function of when it was done. I suspect if the Privacy Act had come into play after we had finished the inquiry it would have contained that.

Senator STOTT DESPOJA—That amendment was moved—let me get that on record.

Prof. Weisbrot—The Northern Territory, which was the last cab off the rank on issues of privacy, freedom of information et cetera does have a specific reference to genetic information in there because of the time frame. We made a number of recommendations aimed at better protection of privacy. One of the central recommendations was in relation to covering genetic samples. That was partly a basic privacy concern. The legislation is very data based, in common with the European legislation; it was an information based database act, and it does not cover samples. However, it does cover things like encrypted CD-ROMs and so on. Our argument was that genetic information, particularly where it has some personal identifier on it, was the equivalent of an encrypted CD-ROM, because you could very easily whack it into the processor and get all of that information out, probably more easily than you could get it out of an encrypted CD-ROM. We thought it should cover that. That was not only important to provide, as a general matter, that level of protection; it also solved a number of other problems for us.

The issue came up often in relation to ownership of tissue that was used in medical research experiments. The ownership issue, as you well know, is a very vexed one when it comes to that

sort of medical research. When we did the consultation around Australia and asked the people who raised these issues, 'What are you really concerned about?' nine times or more out of 10, it boiled down to issues of privacy. They said they were concerned not so much about the ownership but about whether there was access to that information—who would know. There seemed to be a primal fear that, if you volunteered for an experiment in an Australian university and that became a spin-off biotech company, then suddenly that Australian biotech company became an American company. People said, 'Then my genetic material is overseas with no privacy protection and no other protection.'

So we decided to resolve most of those ownership issues in that context through the use of privacy law. We thought that bringing the Privacy Act into the lab in that way, by coverage of samples, would work. I should say we initially had some resistance from researchers, who threw up their arms: they were already overregulated. When we talked to the people who run good labs, though, and we went through their processes, the end result was that they did not have to do anything differently. If you run a good, clean, ethical lab, you keep records properly and you are sensitive to issues of privacy and confidentiality, you would not have to do anything differently. I am sure it is the same in other aspects of industry. If you are doing your job properly, you do not worry about the Privacy Act. But it is to provide a statement of what we expect and to provide the boundaries. In that respect, we thought it was very important that samples be brought in. The then Federal Privacy Commissioner, who was a member of our advisory committee, was a little bit nervous about that in the early stages—not so much about the specific issue, I think, but more about the thin end of the wedge. But, by the end, I think he was really comfortable with the recommendation that we made.

Senator MASON—I have a follow-up from Senator Stott Despoja. How has your report been received overseas? Our government is still looking at it, and I am sure that a report will be produced shortly. Has it been well received overseas?

Prof. Weisbrot—It has probably been the ALRC's biggest hit overseas, in part because the issues involved are so international; it is not looking at an area of local law. It has been used very extensively by Health Canada, which is the department of health there. The OECD working group on human genetic research databases and their working group on genetic testing are both using it very extensively. The Human Genome Organisation's ethics committee and UNESCO's bioethics committee are both referring to it regularly. The Japanese government, the South Korean government and a number of others have referred specifically to it and adopted bits of it. We have been very gratified to see that it has been very influential in that way.

Senator MASON—Congratulations on bringing privacy into the lab.

Senator BUCKLAND—You have almost convinced me to read this report and look forward to your next one!

Prof. Weisbrot—The executive summary is very accessible.

Senator BUCKLAND—I will go to that. I have been listening to what you have said. We can take care of financial things if we have the political will to do it. When it comes to genetic matters and the privacy associated with that and with health related issues, we really cannot legislate for that, in that if you set something in concrete today it changes tomorrow, doesn't it?

If at some point in time—without looking at the ethics of this, because we will start a debate on this side of the table—if there is ever a right of science and medical science to pursue stem cell research further and develop that to use the benefits or perceived benefits, depending on how you want to look at it, then we come to another set of legal boundaries, don't we? We may not know where the stem cells come from—that is, the person—and the relationship between those stem cells and the recipient. I suppose, in another sense, it is the same thing if we look at animal genetics and cereal genetics. It is an ongoing thing: legislation today will not cover it in five or 10 years time. How do you get around that—by using a commission type authority?

Prof. Weisbrot—That was the primary reason for our recommendation of establishing a human genetics commission. We said that, as much as we would like to, we are probably not going to be doing this inquiry every five years—

Senator BUCKLAND—I will read it now.

Prof. Weisbrot—and the generational leaps in knowledge and science and technology in this area are coming every two or three years. It really is extraordinary. People are brainstorming things that they would have said would happen in 20 or 30 years but they seem to be happening in just a few years. We are trying to put in place a general regime that would be robust enough to cover what we understand to be the current state of the science and where it is likely to go. We had on our advisory committee several of the leading geneticists in Australia, people who are being spoken of as potential Nobel Prize winners, so we were getting good scientific advice.

Ultimately we said that human genetics will continue to change and evolve—five years ago no-one knew what stem cells are and now it is a big debate—so we need a human genetics committee or commission to provide government, industry and the general public with state-of-the-art advice about what is happening in the science, and that the committee or commission should also include people who could speak about the ethical, legal and social implications. We said the committee should have a two-strand advisory role—one being the hard science and the other being what that means in terms of ethical, legal and social implications. So we are pleased that that recommendation has taken hold, because the issues that we will face in 10 years will be quite different than the ones we are talking about at the moment.

Senator BUCKLAND—It is amazing. You would know more about this than I, but there was a report in the last few days of a cow that produced, I think, 130 litres in a day, which is almost beyond belief. There has to have been some genetic modification either to the cow or to the feed that they were using to be able to do that. I am wondering about the ongoing implications of that and whether milk produced in that way would have side-effects. It is a minefield.

Prof. Weisbrot—Our report was addressed to human genetics, and our recommendations were in that area. The Office of the Gene Technology Regulator looks at plant and animal stuff. But you are right that genes are not human or animal. Genes accumulate in different fashions and create different organisms. So it may be that at some stage in the not too distant future we will need to have some overarching body that looks at the interlink between the work that the OGTR does in regulating plant and animal experimentation and the work that people need to know about in order to plan best for human health. Our terms of reference limited us to looking at it in a specific way, and in fact our follow-on reference on gene patenting was also limited, fairly artificially but sensibly, to issues of human genetics and human genes. Those issues will

increasingly cross and merge. The NHMRC recently had a big process looking at xenotransplantation. You can see how very quickly these things can move from one area to the other.

CHAIR—Thanks very much. We could go on for a while, but it has been quite valuable and a good promotion of the report. Thank you.

Senator STOTT DESPOJA—Can I get on record that the family law legislation has not been passed; we are still in the midst of debating it. I think I said it had been passed.

[11.39 pm]

CURTIS, Ms Karen Laurina, Privacy Commissioner, Office of the Privacy Commissioner

PILGRIM, Mr Timothy Hugh, Deputy Privacy Commissioner, Office of the Privacy Commissioner

CHAIR—Welcome. Would you like to start with a short opening statement and then we will have more than enough questions.

Ms Curtis—Thank you very much for the opportunity to appear before the committee today. In late February, I wrote to the committee to say that I would not be making a submission to the inquiry because I was undertaking a review of the private sector provisions of the Privacy Act but that I hoped the Attorney-General would release the report—we were to give it to him by 31 March, which we did—in time for your committee to take into account my recommendations and get the benefits of our huge process. I am pleased to say that yesterday the Attorney released the report, which has enabled me to talk at length about the recommendations I have made. So, as an opening statement, I would like to give an overview of the report for you. I recognise that as it contains over 345 pages, although it is not quite as weighty as the ALRC tome, it is a significant report which will take some time to digest.

Firstly, the Attorney gave me terms of reference in August last year that asked me to check on whether the objectives of the Privacy Amendment (Private Sector) Amendment Bill 2000 had been achieved in the first few years of operation of the privacy provisions. Originally when the legislation was going through, the review was to take place after two years. But, as it has turned out, I think it was a great benefit that the review had three years of operation of the act. We embarked upon a very well-developed assessment of the provisions of that private sector amendment act. I created a steering committee and a reference group. We held public consultations in all the capital cities. We received written submissions. I issued an issues paper last October. I asked submitters, within an eight-week period, to get comments back to us. By and large, we received most of those before the end of last year, so early this year we conducted an assessment and analysis of those submissions and talked to other stakeholders.

The essential finding is that on balance the provisions of the private sector amendment act have worked well. I have to say that business thinks they have worked better than consumers think but there was no significant evidence that there was any fundamental flaw with the provisions. However, I have still made 85 recommendations which go to finetuning a number of the provisions, making some higher level suggestions and recognising that there are many actions and activities that my office can undertake to improve the way the provisions are understood by the community and by business. About 30 of the recommendations go to the office streamlining its procedures or improving its guidance.

The recommendations I have directed towards the government are couched in terms of the government considering a number of a things. The biggest issue is national consistency. It has not been achieved throughout the first three years of the operation of the act. It is probably for a variety of reasons: the environment has changed in some ways; security concerns; and the fact

that exemptions under the act, for instance, may have led some states and territories to develop their own laws. I am specifically referring to workplace surveillance in New South Wales, and it is also mooted in Victoria. That is a key issue for us, especially in the areas of health and telecommunications.

Two of the objectives of the original act were to help businesses in the international context. I found that basically our laws have not received European Union adequacy. But in practice businesses have been able to cope with that. They have used contractual provisions to help them with transferring personal information overseas and dealing with European countries. Another area where the original objective has not been met is the development of national privacy principle codes. To date, the office has only approved three codes, and business has not felt the need to adopt codes; it is complying with the law. Originally it was believed that codes would be adopted by business or business organisations. I have suggested as one of the recommendations that we may need to look within our office at reviewing our code development guidelines to make it simpler for business.

So the main recommendation is about national consistency. But I would also emphasise that I think understanding within the community about their rights is not as strong as it should be. Likewise, knowledge in the business community about their responsibilities and obligations is probably not as well developed as it should be across all sectors. I think it has been borne out by the evidence provided to us that the larger businesses—particularly the banks and finance companies which have been dealing with personal information for longer and it is probably more in their interest from a market share perspective to ensure that they handle personal information appropriately—have done better than more medium-sized businesses. So I have recommended that an awareness and education program be undertaken for the community generally, including individuals, and for the business community.

I have recommended that the small business exemption be retained but modified. At the moment the small business operator is defined by turnover of $3 million. That is a bit cumbersome for everybody: for an individual who wants to know whether the person they are dealing with would be covered by the Privacy Act or not; for the business itself that is not quite aware where its turnover is; and for our office, when we are asked to investigate to establish whether there is jurisdiction, it is a little more complex than it needs to be when we look at turnover. I have suggested that the act be amended so that the definition relates to the number of employees, and I have suggested that the ABS definition, which is 20 employees, be used. I think it makes it easier for small business because that one is used more often in that area.

I have also suggested that with those smaller businesses that are higher risk, and I have specifically mentioned internet service providers—tenancy database operators, for instance—the existing regulation-making power under the act be exercised to ensure that they are covered under the Privacy Act. At the moment there is some suggestion that some may not be. Internet service providers hold a lot of personal information about individuals and they of course are covered under the Telecommunications Act. That goes again to one of the problems with national consistency. Under the telco act they are covered; under the Privacy Act maybe they are not.

They are some of the highlights. I would just say I tried to be pragmatic on a number of areas, specifically alternative dispute resolution, natural disasters and large-scale emergencies like the

Boxing Day tsunami last year. Also, for people whose decision making is impaired I have suggested that the Privacy Act could be amended to assist in those circumstances.

CHAIR—It seems that you are saying that it might be working well but it could work a lot better.

Ms Curtis—Yes, and with the benefit of hindsight it is appropriate to make those recommendations.

CHAIR—I will start with a couple of them. You mention the codes and you said to us today that you thought they could be simplified for industry, but you are also recommending that they be made binding.

Ms Curtis—No, that is a different sort of code. The national privacy codes that businesses can develop must include all of the national privacy principles, or at least incorporate the equivalent standard of those NPPs. And then they have to have a code adjudicator process—all of those sorts of things. The idea of the binding codes that we have suggested is to come up in other areas where perhaps they were not going to be voluntary. The NPP codes are developed on a voluntary basis. The ones that were binding could possibly be done for technology, or for an industry that was not working as well—perhaps the tenancy database area.

CHAIR—The other question I will ask at this stage is with regard to the small business exemption. You have identified problems with telcos and ISPs; there are problems identified by the ALRC with health related entities. I wonder whether it would be better to do away with the exemption altogether. Your concern is about simplicity so that people can understand the exemption and know what their rights are, but 20 employees or fewer is going to be hard for people to identify as well. How do you know how many employees are working for a particular entity? Is it best to do away with that exemption?

Ms Curtis—One of the premises of the act is that there be a balance between the individual's right to privacy and the community's needs, and between the free flow of information and businesses operating efficiently. If the small business exemption were removed entirely, there would be a cost to I think it is 1.2 million small businesses in Australia.

CHAIR—Have you made your own assessment as to what that cost might be?

Ms Curtis—No, I have not. There were suggestions in some submissions that it would be over $1 billion.

CHAIR—There are always $1 billion suggestions everywhere! But you did not make your own assessment?

Ms Curtis—No.

CHAIR—Okay.

Senator MASON—Ms Curtis, you referred to the European Union in your opening statement. I am just looking at your review of the Privacy Act and your recommendations. You say:

There is no evidence of a broad business push—

that is, an Australian broad business push—

for 'adequacy'.

That is within the meaning of the European Union trade directives. The recommendation continues:

Given the increasing globalisation of information, however, there may be long term benefits for Australia in achieving EU 'adequacy'.

You go on to say:

The Australian Government should continue to work with the European Union on the 'adequacy' of the Privacy Act and to continue work within APEC to implement the APEC Privacy Framework.

Why would business bother if they can get around it with contracts?

Ms Curtis—It would be simpler for them if they did not have to use contracts for privacy provisions.

Senator MASON—It is as simple as that?

Ms Curtis—I believe that is the case.

Senator MASON—Senator Bolkus and Senator Stott Despoja would know more about this than me, but that is a debate that has been running for years, particularly about trade—that if we did not measure up to these privacy principles our trade would suffer. You both agree with that. The committee has learned that in fact it has not inhibited Australian trade with Europe. I think that was your evidence, as well as that of Ms Sangster from the Australian Direct Marketing Association. It strikes me that it was such a false debate. It was one of the big debates, we had Justice Kirby talking about it and in effect it meant nothing.

Ms Curtis—In practice it has not played out as everyone expected it would.

CHAIR—That is often the case.

Senator MASON—It is disappointing at one level. It is just surprising.

Ms Curtis—I think a lot of businesses, particularly larger businesses, actually thought it would inhibit trade and they were advocating for the private sector provisions to be introduced.

Senator MASON—Earlier on, the Australian Privacy Foundation made an interesting point. They spoke about the moral panic associated with the war on terror and so forth. They said that at some levels the Privacy Act is becoming a bit of a disadvantage because it is being used as a catch-all to show that the government is doing enough to protect privacy—in other words, 'Why

are you worrying about that, because we have a Privacy Act that is looking after those concerns.' What do you say to that? As a politician, it is a great rhetorical defence, isn't it, to say, 'We have the Privacy Act, and Ms Curtis and Mr Pilgrim will look after your privacy?' What the foundation were really arguing was that privacy protections have in fact been whittled away, particularly in the context of September 11.

Ms Curtis—I think we should all remember that, while our Privacy Act is about the protection of personal information or sensitive information, it is really about data protection. It is not about privacy in the broader sense of bodily privacy or privacy in other areas. I think 'privacy' is often seen as a catch-all, and so our Privacy Act does not address all aspects of territorial privacy or bodily privacy. The Privacy Act addresses the collection, use, disclosure and storage of personal information held by Commonwealth government departments and agencies, ACT government departments and agencies and also the private sector across Australia.

Senator MASON—You are right, and it is an interesting question which we could talk about for a while. It is an interesting debate because there is a lot of literature now about the moral panic associated with September 11—you would know this better than me—and about how privacy has been whittled away. You do not need to comment on this, but that or may not be the case. The Privacy Act is not about that anyway. It is really about protecting personal information and data, whereas legislation that the parliament may pass in relation to national security may whittle away privacy in terms of your right to silence or whatever. But that is not really your concern.

Mr Pilgrim—If I may add something to what the commissioner is saying, there will be situations where information may be needed to be passed on to agencies outside Australia—for example, as part of an investigation if it relates to terror. Without some change to legislation, be it through the Privacy Act or through some other specific legislation, it may be that the Privacy Act would stop that information being able to be transferred out in the case of an investigation. You are must better placed of course, Senator, to consider these things. The parliament has to consider where that balance is. Do you then put in a new piece of legislation to allow that transfer to happen, which would then possibly override the protections in the Privacy Act? So it is the issue of the balance. We would say that in certain circumstances privacy cannot be an absolute. There has to be that balance achieved between the needs of the individual and the broader community.

Senator MASON—That is a good answer. Privacy becomes one of those things that are highly contestable—politically contestable. The moral panic associated with September 11 has highlighted that better than anything else. Just think of the rhetorical and political purchase that privacy had in 1987 with the Australia Card debate. It was very strong, very profound and ultimately victorious. I suspect privacy does not today have the same purchase politically or rhetorically that it had then. You do not need to comment on that but, as a politician, that is my sense.

Senator STOTT DESPOJA—Thank you for your report. Obviously it is going to take us a bit of time to plough through some of the content and recommendations. I will just start with a few questions on that. I note that there are a number of matters not included in the review, one of which we have just been discussing—that is, genetic privacy. With regard to employer records,

children's privacy, electoral roll information and related exemption of political parties from the act, I understand that the premise for not investigating some of these areas or reviewing them was the fact that they are the subject of other reviews. Is that the rationale for not investigating the exemption as it relates to political parties?

Ms Curtis—I think that is probably a question that the Attorney or his department is best placed to answer, but my understanding is that there was an amendment in the middle of last year to the electoral roll legislation. I think that was maybe what the Attorney was referring to.

Senator STOTT DESPOJA—As you would be aware, a number of submissions have referred to that particular exemption—in fact, one this morning in quite strong terms, from the Australian Privacy Foundation. So that might be an area where we may have questions on notice, if you are happy to take them after this.

Ms Curtis—Sure.

Senator STOTT DESPOJA—Can you give us an idea of the mix of submissions that you received? I understand that you received a large number of submissions. Could you give us an idea of the balance—how many of those were from consumers and how many of those were from, say, business and industry? That may be a difficult analysis to give us. If it is broken down in the report and you can refer us to that, that would be great.

Ms Curtis—The list of submissions is in an appendix. I cannot, off the top of my head, give you the exact numbers but I was very pleased with the variety of the submissions we received. We did receive individual businesses as well as business organisations, we did receive consumer organisations and privacy advocate submissions, but we also received about 20 from individuals. They raise some very interesting issues.

Senator STOTT DESPOJA—So you are happy with that balance?

Ms Curtis—It was a very rich set of information that we received. It was complemented nicely by all the public forums we held. We have referred in the report to some of the comments that we were given during that process because people are often very open and they said what was really bugging them in that context.

Senator STOTT DESPOJA—Undeniably you have had a large number of submissions but I was just wondering about the mix. That answers my question. No doubt one of these appendices will answer it in detail, because you have got a few.

Ms Curtis—I think it was appendix 3, from memory.

Senator STOTT DESPOJA—In relation to evidence we heard this morning from Baycorp, they put on record—and I do not want to misrepresent them in any way—that they were quite happy with an increased speed in the resolution of complaints. I think that was partly because a lot of the complaints went directly to the commissioner and they either were not aware of them or were not in a position previously to resolve those complaints. I am sure we are all happy to see a much speedier resolution of complaints, and you no doubt—I will get onto resourcing shortly. But does this indicate a culture where it is almost an outsourcing of complaints—that is,

the subject of the complaint is expected to be, or can be, the body that actually handles or helps to resolve the complaint. Is that something we should be aware of or concerned about? Is it appropriate?

Mr Pilgrim—With the processes we handle for resolving complaints, we try to take an alternative dispute resolution process and, where possible, try to conciliate the outcomes of those complaints. The act stipulates that the complainant should try to resolve the issue with the respondent organisation first prior to coming to our office to try and resolve that complaint. The discretion is always there for us, if the individual has a particular reason why they do not want to do that, to ask us to investigate immediately. But I would say that the majority of people will go to the organisation first. I think it reflects a good opportunity for the organisation—who, I would suggest, on the whole want to maintain the best possible relationship with their customers—to do that. We would then be almost a safety net, if things are not resolved properly for them to come to us to resolve the complaint.

Senator STOTT DESPOJA—That is how I envisaged it would operate under this type of regulatory regime. In terms of the practicality, though, does that mean when people come to the Privacy Commissioner first, your first obligation is to ask them if they have drawn it to the attention of that particular body, industry or organisation and then ask them to make that next step? Do you inform the organisation itself that there is a complaint?

Mr Pilgrim—If, for example, a person rings into our hotline to find out how to complain, the first question we would ask them, having determined that it is something that could be covered by the Privacy Act, is whether they have complained to the organisation. If they have not, we would suggest that there is a requirement that they do that, unless there is a good reason they can demonstrate to us why we should immediately take on board that complaint. If the individual who is making the complaint says they will go to the organisation first, then we would not independently contact the respondent organisation at that point. Our first contact with the respondent organisation would occur once we had commenced preliminary inquiries into a complaint that we were possibly going to investigate.

Senator STOTT DESPOJA—That is what I thought.

Ms Curtis—Our figures show that we have about 20,000 inquiries to our hotline a year but last year we only ended up with 1,276 complaints.

Senator STOTT DESPOJA—That 20,000 is quite a number. I noticed somewhere in the recommendations—again, forgive me for not quoting from the exact recommendation—that you talked about having the power, as the Privacy Commissioner, not to further pursue a complaint if it were deemed to have caused minimal harm. Could you talk us through that notion? I think it is in the section about changes in your powers.

Ms Curtis—I think it is page 162. We make it clear that we can decline to investigate complaints where there is little public interest—for example, where there is minimal apparent harm or the matter has been considered before and the organisation, for instance, has already changed its practice. A change in practice would probably have been one of the outcomes that we would have sought from the organisation.

Senator STOTT DESPOJA—So there is no particular definition of what constitutes minimal harm? Obviously, you are taking it into account with those other provisions, but how do you define that?

Mr Pilgrim—It would be hard to define because you would have to look at things on a case-by-case basis, naturally. I can give an example, and it is not meant to sound flippant. We have had the situation where we have had complaints lodged with us from individuals who have gone into a shop and on the face of it they have been denied a receipt for a very small purchase on the basis that the organisation wants to collect some basic information such as their name and perhaps their phone number or their address to validate the purchase. The person said that they did not wish to give the information over and the organisation did not then provide a receipt for the purchase of, say, a $20 item.

Under the act currently it states that, on receiving a complaint such as that, the Privacy Commissioner shall investigate. As you can imagine, that has resource implications if we are looking at that sort of issue. One of the things we would prefer to do is to be able to advise the person that we have received that sort of complaint and will monitor it to see if that is a particular systemic issue and look to see if there is a broader systemic issue over time that we need to resolve rather than having to devote immediate resources to that one particular issue. I am not trying in any way to belittle an individual's complaint—please understand that—but that is just an example of an instance where there is something that you probably would not want to devote an entire person to trying to resolve that at that point.

Senator STOTT DESPOJA—Thank you for that explanation. You mentioned the word 'resources'. One of the public comments that have arisen out of this report from you, Ms Curtis, is to do with the desire and need for further resources. Can you advise the committee on what kind of resourcing you are referring to? Have you got figures as to how much money you would need in order to deal with some of the issues that you and others have identified, including a backlog in resolution of complaints et cetera? What kind money are we talking about, or is that not something that you have put a figure on?

Ms Curtis—It is clear throughout the report that there has been a call by all sectors—business large and small, individuals, consumer representatives—for increased resourcing for the office in terms of our complaints handling and also for an education and awareness program. I have made recommendations to the Attorney that he should take into account those strong calls for increased funding for those areas in particular. We have not developed an education and awareness program, so we have not costed what that might be, so I cannot give you a specific figure.

Senator STOTT DESPOJA—Obviously this report now is in the hands of the Attorney-General; have you been given a specific time frame for his response?

Ms Curtis—No, I have not been given a specific time frame. It is not like three months for Productivity Commission reports or Senate reports, for instance. But we expect that the Attorney will be wanting to respond as soon as possible. It does affect a number of portfolios, so it will require getting a number of departments and agencies and then ultimately ministers together to determine that whole-of-government response.

Senator STOTT DESPOJA—So does the ALRC report, but we have been waiting since 2003. I am just wondering whether you have a preference for a response within a certain period of time.

Ms Curtis—I would love for the report to be responded to as quickly as it can be by government, because the recommendations we have made will improve the operation of the act and so I think that it is important that they respond as soon as they can.

Senator STOTT DESPOJA—Moving beyond your report specifically: have you been asked by the government, by Attorney-General's or other ministers and their departments, to provide information or advice on some of the proposals, including biometric passport information, smart cards or the new health card? Have you been invited to provide a view on these particular issues that clearly have privacy implications?

Ms Curtis—Yes, we have. One of the statutory responsibilities is to provide advice to government on policies and proposals as they are being developed. So on smart cards we have been asked for advice. On biometrics, we have been funded in the budget to work with Customs and DIMIA and DFAT. And on identity security we are working with the Attorney-General's Department in their process of document verification and other areas, and we were funded in the budget for that as well.

Senator STOTT DESPOJA—Have you expressed some concerns to government about some of these areas?

Ms Curtis—Again, as the statutory responsibility is to promote privacy and also to provide advice, my office has been expressing a number of views about some of the proposals. We always look at the balance that is required, the need to understand the basic principles of privacy about consent, for people to understand what information is being collected about them, how it is being collected and why—for what purpose, how it will be used and disclosed. We often say that trust is so important to any of these proposals, so full disclosure and transparency are very important aspects of the development.

We have advised that departments should consider a privacy impact assessment process whereby they examine any new policy proposal in the light of the impacts on a person's privacy, and that, each step along the way, they should continuously look to see what it is they are proposing to do and whether it is the best way. Things can be done in a privacy-enhancing way rather than an in a privacy-intrusive way. As we often say, the biggest invasion of a person's privacy is that their identity is stolen, so we need to address some of those issues.

Senator STOTT DESPOJA—Do you feel that your concerns or your advice in relation to, say, the biometrics aspects of the recent passports legislation that was passed last year were taken into account appropriately?

Ms Curtis—I think we provided those comments before I took on my role.

Mr Pilgrim—The comments we provided were certainly taken on board. My memory not being that good at the moment, I could not say exactly which ones were picked up and which

ones were not, but we were certainly involved in those discussions and given a lot of opportunity to provide our comments on that legislation as it was developed.

Senator STOTT DESPOJA—My next question relates not so much to those aspects I have just referred to that may actually have a legislative form already or are about to but to microchip legislation. Are you involved in or have you been monitoring this debate? We have heard reports that the FDA in America has approved the use of microchips in humans. Is this something the Australian government and regulatory scheme are going to have to deal with?

Ms Curtis—We have not provided any advice to any Australian government about microchips. One of the clear principles that underpin our Privacy Act is technology neutrality, so we would like to think that the Privacy Act would be able to apply to some of these things. But in my report I am actually recommending that there be a wider review of the definition of personal information, because the principles are based on essentially 30-year-old notions. So I think down the track it will be appropriate for us to consider all of these issues. Technology has obviously developed so much in the last 30 years and will continue to do so.

Senator STOTT DESPOJA—Picking up on one other statement you made in response to my question about political exemptions: you have acknowledged that you have had complaints in relation to use of personal information by political parties. Are you able to take on notice or tell the committee now how many people have complained to you about the operations or the behaviour of politicians or political parties in Australia?

Ms Curtis—We do have a figure.

Senator STOTT DESPOJA—It is in the report?

Ms Curtis—No. Timothy is just going to pull it up, I think. If we cannot find it quickly, we can provide it to you.

CHAIR—That might be the best way to do that. Senator Buckland has a question or two while Mr Pilgrim ploughs through that.

Senator BUCKLAND—In one of your recommendations—recommendation 26—regarding direct marketing and education, but more particularly education, you say:

> The Australian Government should consider specifically funding the Office to undertake a systematic and comprehensive education program to raise community awareness ...

I put it to the direct marketing people this morning that in fact they could contribute to that as well. What is your response to that? They are the beneficiaries of much of this, aren't they?

Ms Curtis—The direct marketing sector is not the only sector that is covered by the Privacy Act.

Senator BUCKLAND—I am not referring just to them but I did put it to them that they might like to contribute.

Ms Curtis—Throughout our consultation process and in some of the submissions, a number of businesses made the comment that it was a role of government to fund that education and awareness program. I think it was Business SA who said they felt that their members were having to educate people about their rights and that it was not the role of business to educate people about rights; it was a role of government.

Senator BUCKLAND—You do not surprise me that it came from that source. That is a nonsense in reality, isn't it?

Ms Curtis—I think many businesses provide privacy notices and they are providing information to individuals about how they are handling the information, but a wider community program that showed privacy notices on buses and TV would be something that is in the public interest and for the public good, so it is probably better funded by government.

Senator BUCKLAND—In the options reform, the report says:

Businesses around Australia have invested considerable resources into ensuring they are privacy compliant and are calling for improved community awareness.

I understand they are spending money to comply, and rightly so. We expect that. I come back to what I said initially. They are now saying, 'You'—meaning government—'go and educate them.' I find that somewhat hypocritical despite the good office of Business South Australia. As I say, it did not surprise me that that source was mentioned.

Ms Curtis—I think it is a view that is held by some businesses that they would like their actions supported by a government advertising campaign or a program to help raise awareness about individual rights. I am just repeating to you what they have said to us rather than saying it is right or wrong. They are arguing that they are spending resources on it and having to explain it to people. The cost of explaining it to people is a cost they would rather not bear.

Senator BUCKLAND—Or they can simply say, 'We don't have to tell you where we got your name from,' when they phone you up at seven or eight o'clock at night to try and entice you to their services. That is academic.

CHAIR—There is an answer to come back to us.

Mr Pilgrim—In the financial year 2003-04, we closed three complaints on the basis that they were exempted by the political exemption. In regard to that seemingly being a very low number, if people ring in and inquire about whether they should lodge a complaint, if it sounds on the face of it over the phone and we can determine it, we would tell the individual that there is a political exemption and more than likely we would not be able to investigate. I have just done a quick look at the numbers, and we had about 20 phone inquiries in the current financial year in regard to the political exemption.

Senator STOTT DESPOJA—Can you tell us if any of those were sparked by the federal election campaign, in particular the use of people's telephone numbers for campaign purposes and the leaving of messages on answering machines?

Mr Pilgrim—I could not say on the basis of the information here that that was what prompted those calls. We could do some checking, but I am not sure that our system would have caught that information.

Senator STOTT DESPOJA—I would be curious to see if your system has caught it, given it is the recent financial year. It would be interesting given that we have this wide ranging and, as someone said today, an unconscionable objection. I am wondering what kinds of things political parties and politicians are doing with the information that we have at our disposal. There are obviously people complaining, so it would be nice to know what we do with those complaints.

Ms Curtis—In one of the appendices of the report, on page 328, from 21 December 2001 when the legislation came into effect to 31 January 2005, we closed 24 per cent of total complaints—and there were 3,575 of those—as being out of jurisdiction. On the pie chart below 0.4 per of that 24 per cent, which is 24 per cent of 3,575, were political exemption.

Senator BUCKLAND—In appendix 14, you have graphs there that show people who 's. agree', 'agree', are unsure, 'disagree' and 's. disagree'. What is the 's' for? I might be ignorant—I probably am—

Ms Curtis—It means 'strongly'.

Senator BUCKLAND—Why didn't I think of that?

CHAIR—On that note, thank you very much.

[12.20 pm]

LYNCH, Ms Philippa, First Assistant Secretary, Information Law and Human Rights Division, Attorney-General's Department

MINIHAN, Mr Colin, Principal Legal Officer, Information Law Branch, Private Sector Privacy, Attorney-General's Department

WARD, Ms Janine, Acting Assistant Secretary, Information Law Branch, Attorney-General's Department

CHAIR—I welcome witnesses from the Attorney-General's Department. I know we cannot ask you about policy, which may, in light of the previous submission and the report, make it difficult to ask you about much today. But would you like to start off with a short opening statement?

Ms Lynch—We do not have an opening statement, but we would like to thank the committee for accommodating us and having us on today instead of tomorrow.

CHAIR—That is okay. We will start with questions.

Senator STOTT DESPOJA—I understand the constraints before us. Can you confirm that the government's response to the ALRC report *Essentially yours* is still before the Standing Committee of Attorneys-General?

Ms Lynch—I understanding that the parts are with SCAG are the ones that relate to the use of genetics for forensic purposes. They are before SCAG and the police council. I think that is what Professor Weisbrot was referring to. So the whole report is not with SCAG but I think the forensic evidence use is before SCAG, which I think was also the recommendation in the ALRC report.

Senator STOTT DESPOJA—Thank you for clarifying that. Can you tell us where the rest of the report is, to the extent that you can say?

Ms Lynch—The timing of the final release of government responses is of course a matter for ministers.

Senator STOTT DESPOJA—Of course.

Ms Lynch—A considerable amount of work has been done and there are certain clearance processes that need to be gone through. As Professor Weisbrot mentioned, there are a number of ministers and agencies that have some involvement in that. I cannot give you a specific date but a considerable amount of work has been done in putting together a response.

Senator STOTT DESPOJA—But you can confirm, though, that the report has been looked at and analysed in various parts of government.

Ms Lynch—I can certainly confirm that.

CHAIR—Has it gone to cabinet yet?

Ms Lynch—I am not sure that I can answer that, but a number of ministers have been consulted in the process.

Senator STOTT DESPOJA—I had the impression that it had been to cabinet, but obviously you cannot confirm that.

CHAIR—You can take it on notice.

Ms Lynch—I will take it on notice. I am not quite sure what the parameters are of us answering questions about cabinet.

Senator STOTT DESPOJA—Certainly. I am going to try asking the questions, and I totally accept it if you say you cannot answer them.

CHAIR—We will not ask you how many times it has gone to cabinet.

Senator STOTT DESPOJA—In relation to responses to reports, do you have any specific information as to a time frame for a response to the Privacy Commissioner's review that we have just been discussing?

Ms Lynch—No. As the Privacy Commissioner has said, I do not think there is a specific time that the Attorney has in mind for responding. Again, we have already started consultation with other departments. There are a number of departments who have a close interest in a number of the commissioner's recommendations. So that process has begun. We have not been given a specific time in which to have a response ready, but clearly it was a report commissioned by the Attorney and one in which he has a close interest.

Senator STOTT DESPOJA—In the recent budget and in the budget papers, I note that tens of millions of dollars are allocated to projects that have privacy implications—for example, biometrics. In fact, those tens of millions do not even include the $128 million to deal with the new health care smart card or whatever you want to call it. I am wondering what resources were allocated in this year's budget to the Privacy Commissioner. Does it represent an increase?

Ms Lynch—I have some figures here that I am happy to go through. From the PBS the total appropriation to the Office of the Privacy Commissioner for 2005-06 was $4.1 million, which is an increase of $226,000 from 2004-05.

Senator MASON—What percentage is that?

Ms Lynch—I am sorry, I do not have that listed as a percentage. I can take that on notice and get back to you.

Senator STOTT DESPOJA—We can do the math; can't we?

Ms Lynch—The commissioner also estimated revenue from other sources in the PBS. That $4.1 million includes the first year's instalment of the $700,000 that Commissioner Curtis referred to as well. In addition to that appropriation of $4.1 million, out of the $5.9 million that was allocated to the identity security project over 18 months the office will receive $225,000 for providing advice on work relating to that.

Senator STOTT DESPOJA—So that $225,000 is to provide advice in relation to the identity security programs?

Ms Lynch—Yes.

Senator STOTT DESPOJA—And what would that $225,000 assist with? Is that paid in total to the Privacy Commissioner's office and they can determine how they spend that?

Ms Lynch—How that money would be used would be a matter for the commissioner, but it is allocated to allow the commission capacity to provide advice on the proposals and the work that was being done as part of that strategy and the two pilot programs that were specifically referred to in the budget papers.

Senator STOTT DESPOJA—So they could spend that on salaries if they wanted to?

Ms Lynch—I would think so, yes.

Senator STOTT DESPOJA—You would not get a lot of consultants for $225,000. So that is the only additional allocation that deals specifically with the Privacy Commissioner providing advice on those particular matters?

Ms Lynch—There is the $700,000 that relates to the biometrics and border control. That is over four years. Then there is an additional $225,000 over 18 months on the identity security pilot programs.

Senator STOTT DESPOJA—In the review that the Privacy Commissioner has just launched, the rationale for not dealing with a number of issues, including genetic privacy and specifically the exemption that relates to political parties, was the fact that, as I read the report, some of these issues are already subject to review. Can you tell me what review of the political party exemption is being undertaken at the moment?

Ms Lynch—There was the review of access to the electoral roll which was carried out by the relevant parliamentary committee, the name of which escapes me at the moment, but in relation to political acts and practices I would have to take that on notice.

Senator STOTT DESPOJA—I am curious to know if there is a specific review that deals with that. I am not quite sure why it was exempt from the review by the Attorney-General in the terms of reference. One more thing, and this relates to evidence that the committee heard—indeed, it sounds like there is a recommendation in the report from the Privacy Commissioner on this—on the release of information during some kind of national disaster. I note that the Attorney-General made public comments yesterday in relation to that specific recommendation. Can you outline for the committee what work, if any, has been done on that issue before now?

Ms Lynch—I have not seen the transcript of what the Attorney-General said in the press release yesterday, but I can tell you that there is a committee of officials from a number of government agencies looking at the issue of the exchange of information post a major disaster such as the tsunami disaster on Boxing Day. A group of government officials from a number of departments have been looking into that issue for some time.

Senator STOTT DESPOJA—I do not think there was anything specific in Minister Ruddock's press release, but certainly I saw some comments on the wire yesterday. I am happy to take that up at a further time.

Ms Lynch—Certainly work is being done in looking at the Privacy Act and issues arising post that sort of major catastrophe.

Senator MASON—Ms Lynch, one of the interesting paradoxes of public policy is that sometimes you need to place some pressure on the government for them to respond with a wide-ranging legislative framework, and until that time often issues are not progressed. The Privacy Act implemented in 1988 was a response partly, of course, to the Australia Card debate. We have heard over the last couple of days and probably will hear tomorrow in Canberra—and Senator Stott Despoja has mentioned many today—about all these potential impingements of technology on privacy. I note too that in the Privacy Commissioner's report—the secretariat just pointed this out to me—recommendation 1 was:

The Australian Government should consider undertaking a wider review of privacy laws in Australia to ensure that in the 21st century the legislation best serves the needs of Australia.

There are threats, and there were perhaps threats with the Australia Card regime, but just because there are threats does not mean that things get worse. Often in the coming together of a comprehensive framework you can actually prove things. I wanted to know the government's intention with respect to privacy laws. Are you aware of any general intention to review privacy laws?

Ms Lynch—The government will be considering the Privacy Commissioner's report, in particular recommendation 1, which talked about a broader review, and that will be a matter for government to respond to.

Senator MASON—All right. I did not think you would be able to answer it specifically but I just thought I would raise it. There is one issue regarding trade with the European Union, and I raised this with the commissioner before. You may have heard—I think you were listening, Ms Lynch—that I was a bit shocked to hear that no-one really cared anymore, because the private sector has got around the difficulties that were raised so much in the eighties about the European Union not wanting to trade with Australian companies because our privacy legislation was not sufficiently comprehensive. The Privacy Commissioner, however, did say that if our legislation was changed to be more congruent with European Union legislation that would assist—I do not want to verbal you here, Commissioner—the private sector. Is the government currently negotiating to do that?

Ms Lynch—We continue to have discussions with the European Union on a couple of fronts, including on the adequacy of our legislation. I think it might be best for me to defer to Mr Minihan, who has been working on that in the department.

Mr Minihan—As Ms Lynch says, we are still negotiating with the European Union. There is increasing understanding on the part of the European Commission of how Australia's privacy laws work. From the opinion that the article 29 committee gave on Australia Day 2001 which was critical of our laws, there were nine key matters. They now seemed to have recognised that a lot of those matters have been dealt with via some minor amendments we made in 2004—there were four minor amendments—or because they have understood more fully how our regime works. Being a Commonwealth system, there are several law systems, so there has been some learning process going through.

The last contact we had with them was in October last year in relation to general adequacy for the Privacy Act, and they did not raise any new or significant objections. I think their view is that this is something that has been on their agenda for quite some time and they would quite like to have the situation resolved as well, and the commission view seems to be resolved in a positive way. We are talking to commission officials, not the commissioners themselves or data protection commissioners, and I think the prospects are good in the medium term.

Senator MASON—Are the European Union seeking legislative changes to our framework or are they seeking simply process or administrative changes?

Mr Minihan—The commission do not seek any changes. They just say, 'This is what is required for adequacy. This is our opinion.' What we do with that is for us. So I would not want to say that they are directing us to make changes to our laws.

Senator MASON—In your opinion, do we need further legislative reform to become adequate within the EU directives or are there administrative measures we could take that would suffice?

Mr Minihan—We did make minor amendments to the Privacy Act. There were territorial limitations upon the jurisdiction of the act in relation to the way it worked. It would only apply to Australian citizens rather than anybody. So a European who was in Australia and had information collected by an Australian government department could not then have it corrected. Those kinds of minor changes were made to the act. They are the kinds of things which were sensible to do, in any event.

Senator MASON—In the government's opinion, however, will it be necessary, to become adequate within the EU's directive, to seek to implement legislative reform? That is a direct question.

Mr Minihan—Yes. One of the concerns that the European Commission had was the small business exemption, so the government's policy is that the exemption remains. That is probably the key outstanding issue for how that is resolved between the Europeans and Australia. I note that the commissioner has made recommendations about that as well. We will obviously be passing the commissioner's report to the commission soon.

Senator MASON—Are there any concerns about the political parties exemption?

Mr Minihan—Off the top of my head I cannot say, Senator.

Senator STOTT DESPOJA—I have one last question in relation to the online document verification service. Obviously we have seen media reports and recent comments. I am wondering if your department has been involved in providing any advice on the privacy implications of that proposed reform.

Ms Lynch—The document verification service is a project that is being run and coordinated by the criminal justice part of the department. So the privacy part of the Information Law Branch has been involved in that project. It is being run within the Attorney-General's Department with other agencies having involvement as well. It is being coordinated through A-G's.

Senator STOTT DESPOJA—Is providing advice on the privacy implications of that, whether by your branch or others, something you can advise us of now or perhaps take on notice?

Ms Lynch—Certainly the Information Law Branch is involved in a number of aspects of the work that is being done, as is the Privacy Commissioner, in relation to that identity security framework that is being talked about. I think there are a number of subcommittees and groups within the agencies that are working on it. The Information Law Branch, I think, is represented and attends meetings on all of those. So we are having privacy input and are being involved along the way.

CHAIR—Thank you. It has been a bit hard this morning, given yesterday's report, but I am sure we will get another chance in a few weeks time.

Ms Lynch—On Monday at estimates.

CHAIR—Thank you and thanks to all the witnesses who have helped us this morning and who have made submissions.

Committee adjourned at 12.37 pm