COMMONWEALTH OF AUSTRALIA

Official Committee Hansard

SENATE

LEGAL AND CONSTITUTIONAL REFERENCES COMMITTEE

Reference: Privacy Act 1988

FRIDAY, 20 MAY 2005

CANBERRA

BY AUTHORITY OF THE SENATE

INTERNET

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

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

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

SENATE

LEGAL AND CONSTITUTIONAL REFERENCES COMMITTEE

Friday, 20 May 2005

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

Substitute members: Senator Mason for Senator Scullion and 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, Ludwig, Mason, Payne 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 8.59 am.

MORGAN, Ms Stacey, Executive Officer, Administrative and Domestic Law Section, Legal Branch, Department of Foreign Affairs and Trade

NASH, Mr Bob, Assistant Secretary, Passports Branch, Department of Foreign Affairs and Trade

SMITH, Mr Rod, First Assistant Secretary, Public Diplomacy, Consular and Passports Division, Department of Foreign Affairs and Trade

WHITE, Mr Adrian, Manager, Passports Act Review Team, Passports Branch, Department of Foreign Affairs and Trade

CHAIR—Welcome. This is the third hearing of the Senate Legal and Constitutional References Committee inquiry into the Privacy Act 1988. The inquiry was referred to the committee by the Senate on 9 December 2004. It is being conducted in accordance with the terms of reference determined by the Senate. The committee has received over 45 submissions to this inquiry. 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. The committee has been asked to consider a number of aspects related to this purpose.

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. We prefer that all evidence be given in public. Under the Senate's resolutions, witnesses do have the right to request to be heard in private session. It is important that we be given notice if that is the case.

You have lodged a submission which we have labelled No. 39. Do you wish to alter or amend it, or would you like to start off with an opening statement?

Mr Smith—No, we have nothing to add to our submission and there are no additions to that by way of opening statement.

CHAIR—We are conscious that we cannot ask you for your personal opinions on matters of policy. On that basis, we can proceed to ask some questions about your submission. I will start by asking: what is the current status of the introduction of the electronic biometric passports? Is it going ahead? There have been some reports that it might be postponed. Can you give us an update?

Mr Nash—Yes. We are currently proceeding on the basis that the e-passport will be ready for roll-out in October this year, that deadline having been set by United States legislation. That legislation relates to the need to have biometric identifiers in passports in order to remain in the Visa Waiver Program.

CHAIR—That deadline has been set by which legislation?

Mr Nash—The United States legislation.

CHAIR—That does not have effect in Australia, does it?

Mr Nash—No, it does not, but it has always been one of the determining factors in terms of the time frame that Australia has adopted—that is, to meet the requirements of the US legislation to have e-passports in place by 26 October this year. There has been some discussion about whether that deadline might be extended, but it is only that at this stage. There has not been any further decision made.

CHAIR—Is there a provision of the Australian legislation that empowers this, or is that not necessary? Has it been done by regulation or by legislation?

Mr Nash—The new Passports Act that comes into effect on 1 July enables the use of new technologies in passports.

CHAIR—In this particular instance, can you tell us to what extent there has been a privacy impact assessment?

Mr Nash—There have been two privacy impact assessment projects conducted so far. One was done prior to the introduction into parliament of the legislation. That was done last year. That privacy impact assessment of course included the provisions relating to the introduction of biometric technology into Australian passports. And there is currently a biometrics- or e-passports-specific privacy impact assessment being prepared.

CHAIR—Who is doing that?

Mr Nash—We are doing that internally in consultation with privacy advocates and the Privacy Commissioner.

CHAIR—Is the consultation broader than that? Are you involving public submissions, for instance?

Mr Nash—No public submissions have been obtained except from those advocates that I mentioned, although the opportunity has been made available through the advertising last year of the fact that there was room for public consultation. This was also mentioned during and prior to parliamentary debate on the issue.

CHAIR—There has been one specific concern—amongst others, I suppose—that the chip that is proposed to be inserted into the passports does have some dangers, in that it may be able to be read remotely and so on. That has come from the Australian Consumers Association. Have they had a chance to be consulted on this, and do you have any considered view on the chip and its capacity to be read?

Mr Nash—We are very aware of the concerns of not only privacy advocates but a number of others within the community, in Australia and internationally, particularly in the United States, about this possibility of eavesdropping—the illegal reading of passport data contained on microchips—or skimming, as it is commonly known. We have looked at this quite extensively

and our testing to date has failed to prove that it is a possibility, frankly. But it remains a very strong perception and we have taken the view that, in the longer term at least, it will be possible to do it. So to mitigate that possibility we have decided to introduce a coded arrangement, called basic access control, which will require that the machine-readable zone on the data page of the passport be read in order to unlock the chip—in other words, the data on the chip will be protected and will not be able to be read unless that pin is used to unlock it.

CHAIR—And that is secure? How secure?

Mr Nash—It is very secure. The other options are rather cumbersome—things like putting metal into the covers of passports. Another possibility that has been discussed is total encryption, which is simply impractical. If you encrypt data, then obviously you have to de-encrypt it. That would mean that every country in the world that adopts this technology would require the code to unlock the data that is contained on that microchip.

CHAIR—In terms of the chip, what sort of information will it contain?

Mr Nash—Only the information that is currently shown on the data page. The suggestion that biometric data is something different is probably one of the greatest misunderstandings in relation to the introduction of this technology. It is simply what we now have on the data page of the passport. The only difference is it is written to the chip as well.

Senator STOTT DESPOJA—I would like to start with that last point—the idea that it is exactly the same as what we currently have. At the moment, we have a passport where people can compare a face or an image. The difference with this biometric data is that it will be affected, as I understand it, by changes in surgery or ageing. In terms of the biometric data reading that image, is that not affected in some way by changes in a person's appearance, including ageing? Isn't that one of the faults of the system at the moment?

Mr Nash—I am not sure I would call it a fault. It is, of course, correct that, with ageing, simple things like hair covering foreheads, beards and glasses and so on can have impacts on this technology. I think the important thing to note is that we have done a lot of testing with regard to those issues. Because this technology is based on what we call eye coordinates, we have been able to do a lot of work within the software to ensure that we can get matches about 98 per cent of the time. As far as the other two per cent are concerned, all that happens, if somebody has got older and cannot be matched, is that they will simply be referred to a secondary processing at airports, for example, to ensure that they are who they claim to be. I think there is some misunderstanding that individuals will suffer as a result of perhaps not having been matched. We have had extensive consultations with the United States and a number of other countries about this issue through the International Civil Aviation Organisation. It is generally accepted the way those people will be processed is simply the way they are processed now. The data on the microchip is designed to facilitate the processing of people through matching.

Senator STOTT DESPOJA—I am not suggesting, of course, that growing old is a fault; I was just checking the efficacy of the system. Following on from Senator Bolkus's opening question, I do not think there is much contention that we have to meet international standards in relation to our passports and getting up to speed. I do not think that is an issue. I am curious though—and this is where the contention seems to be—in relation to security and/or privacy

and, secondly, in relation to the data sharing. Why is there an allowance for extensive data sharing with other government departments under the legislation? Why is that necessary?

Mr Nash—I will begin by defining the term data sharing. There is some misunderstanding about this concept as well. A lot of the responsibility for this is outside our portfolio. A lot of this exchange-of-data discussion going on at the moment is principally within the Attorney-General's Department and among a whole bunch of agencies. But, as far as protecting our data is concerned, what is being proposed here is a verification system ensuring that the data we have in our database is the same as it might be in other databases—for example, the registrar of births, deaths and marriages in a particular state would have a clear interest in ensuring there is a match between the identities in our database and theirs. It is not a simple matter of suggesting that a particular registrar would have unfettered access to our database; it is more a matter of their being unable to confirm somebody's identity within ours through the provision of minimum information.

Senator STOTT DESPOJA—We heard evidence yesterday from the Australian Privacy Foundation. They described the situation that is developing in different countries with increased collection of data by governments or anyone else—and this is not specific to passports—as a 'honey pot to bear' scenario. They thought that systems that have increasing, centralised and concentrated amounts of information on an individual might provide a greater incentive for people to hack into that system. Do you think that is a possibility? What security arrangements are in place? You are talking about a database potentially of biometric images of the faces of all Australians. You can understand why people might be concerned by that.

Mr Nash—I can certainly understand the concern. I think, though, that it comes back to the point that what is being proposed is nothing different, really, to what exists currently. There is no more data involved in the e-passport process. There is no more data held centrally on Australian citizens than there is currently. We currently have biodata. We have all of the personal details of Australian passport applicants. We currently have images on our passport databases. Those things would remain under the e-passports project. As I said before, the exchange of data, which probably should more correctly be termed the verification of data held in different databases, does not involve any extension of databases or the creation of a massive database; it involves the validation of one set of data against another.

Senator MASON—You mentioned in your submission that the Privacy Act may be an impediment to the sharing of information following an overseas crisis. I suspect the tsunami crisis of recent times is a good example of that. To be fair, the Australian Red Cross gave evidence to us in Melbourne about the same issue. Could you elaborate on that, please? What are the impediments? Have you asked the federal Privacy Commissioner to do anything about it?

Mr Smith—Let me answer that perhaps by illustrating some of the issues that we addressed when we were managing the tsunami crisis in December and January. We had about 87,000 phone calls from members of the Australian public expressing concern about the whereabouts of family members and friends. From that, we developed a list of about 14,000 Australians who we judged may have been in the areas affected by the tsunami. Tracking down 14,000 Australians and confirming their safety is an extremely difficult task. It is one that we could not do on our own. It was very important that we were able to get as much information as we possibly could about where those individuals might have been at the time to help us to get a clearer picture

about the risk that they may have been in the immediate vicinity of the tsunami. On the whole, that process worked pretty well. There was generally good sharing of information between government agencies.

One of the critical sources of information we had was information from the Department of Immigration and Multicultural and Indigenous Affairs, from their entry operations area. It was able to tell us when Australians had returned to Australia. So all of those that we knew had come back safely but who may not have been back in touch with the family members or friends who reported them to us in the first place, or who themselves reported to us that they were safe, we were able to cross off our list of 14,000 people. So we got that information from Immigration and there were other sources of information as well. We got to the point after a while, when we had exhausted all of the sources that we had in the Department of Foreign Affairs and Trade, when we referred names to the police—and I mean through the AFP to the missing persons units in the various state and territory police forces—so that they could then use the resources that they have to follow those things up.

The biggest impediment we found was getting access to airline information that could potentially have been very useful to us in narrowing down the movements of the individuals that had been reported to us. There were constraints. There were limitations placed by the Privacy Act on the provision of that information by those private agencies. There were also some—'impediments' may be too strong a word—limitations to information that could be exchanged between government agencies. They generally could be managed. As I said, the information flow between government agencies was pretty good, although it was not always as quick as we would have liked. We needed to ensure that the appropriate authority required under the Privacy Act for the provision of information between agencies was there, so letters had to be written—we had to get proper legal advice that provision of information was covered.

The real issue, though, was getting information from private sector organisations, particularly airlines and travel agencies. That is something we are looking into now. There is a working group process, being led by the Attorney-General's Department, looking at the extent to which new flexibility needs to be built into the act or into the application of the act to help us with the management of information with privacy issues in times of crisis.

It is a slightly more complex issue getting information from the private sector, because they operate under slightly different privacy principles to those for government. We are working through that now, and we will obviously be working very closely with the Privacy Commissioner in doing that. We do have not a resolution to that yet, but that is something we are following up.

Senator MASON—You will be pleased to know, Mr Smith, that one of the issues that the committee has looked out over last few days is whether the privacy principles that apply to the private sector should be the same as those that apply to the public sector. That is one of the issues we are looking at. Nonetheless, that is down the road a bit. Just be aware that in times of crisis, sure, information sharing perhaps facilitates rescue and so forth, and citizens back home and relatives feel better because they have more information about their relatives. But one of the issues we discovered in our examination of the Red Cross was that when the Australian Federal Police becomes involved as a law enforcement agency it is difficult to divide their role between their humanitarian work, which I think we all acknowledge is considerable in times of crisis, and

their law enforcement work. When they are given information in their capacity as a humanitarian organisation—in effect, helping with identifying bodies and so forth—

Senator PAYNE—DVI.

Senator MASON—Yes, all that sort of stuff—that is terrific. But, on the other hand, the information of course cannot then be used in their law enforcement. In a sense you are asking one particular body to have two different personalities. That is a difficult situation to overcome.

Senator PAYNE—In your tens of thousands of phone calls and in your interaction with that many Australians, what was the sort of reaction that you were experiencing from the general public about your inability, because of the privacy restrictions, to access the sort of information that may have been helpful?

Mr Smith—It was not a particular focus of our interaction with members of the public at that time. We were doing everything we could to track down their friends and loved ones. In circumstances where we had ongoing contact with, say, a particular family and we had been unable to locate the individual, we would have a pretty frank discussion with the members of the family seeking their assistance to get additional information about the things that their missing loved one might have been doing—for example, accessing bank accounts. That could give us a clue as to an individual's whereabouts and whether or not they were still alive.

People understood that. Members of the public understood that we were very careful about privacy, and they would do what they could to help. In a lot of cases they would go to the loved one's bank, and the bank would refuse to give the members of the family access to their bank records or even to confirm whether or not a bank account had been accessed. So I think people are pretty understanding about it all. Of course, this was all done in a climate of great uncertainty, distress and concern. But, on the whole, people were generally pretty understanding.

I might add—to pick up Senator Mason's point about how personal information is managed within a police force—that not all of the 14,000 names that we had were provided to the police. A much smaller number were provided to the police, because we passed the information to the police after we had been through a process of culling. Of the lists that were provided to the police, we had only one complaint from an individual that his information had been provided to the police.

Senator PAYNE—That goes directly to the question I was asking as well.

Senator MASON—Of course that would have drawn attention to himself as well.

Mr Smith—We do not know the nature of his concern, but I think it was just somebody who had a very strong sense of his own privacy and was concerned. Obviously I will not go into the details, but his name had been given to us from two quite independent sources. The prudent thing for us to do when we were able to get no further information about that individual was to seek the assistance of the police.

Senator MASON—As you say, the big difference here is between information sharing between public government agencies on the one hand and the private sector on the other.

Mr Smith—Yes.

CHAIR—Thank you very much for your submission and your assistance this morning.

[9.24 am]

CHALMERS, Professor Donald, Director, Centre for Law and Genetics, University of Tasmania

NICOL, Dr Dianne, Senior Research Fellow, Centre for Law and Genetics, University of Tasmania

Evidence was taken via teleconference—

CHAIR—You have lodged a submission, which we have numbered 24. Do you wish to make any alterations or amendments to it?

Prof. Chalmers—We would like to make some comments at the end which are not contained in the submission, in relation to developments in data linkage for research purposes.

CHAIR—Would you like to start off with an opening statement?

Prof. Chalmers—Yes, very briefly. We have tried to answer the questions set by the committee. To highlight, we hope that we have stressed, first of all, the continuing need in this country to integrate the federal and state privacy legislation, though unfortunately there are still gaps in the way in which the privacy legislation is organised. Secondly, we have obviously had dealings with the Australian Law Reform Commission and the Australian Health Ethics Committee report entitled *Essentially yours: the protection of human genetic information in Australia 2003* into genetic privacy. We believe that that is a sensible approach to integrating genetic privacy into the general privacy law, rather than having a separate act. However, we do note that it is possible, as we said in our submission, that as a nation we may start to move towards health privacy legislation. Thirdly, we have tried to highlight the growing use of human tissue in research and the need to integrate that into the privacy framework—recommendation 8.1 of the *Essentially yours* report suggests that that be described as sensitive information, and we believe that is sensible.

Fourthly, we are concerned about the rather soft touch enforcement of privacy. We think that there has been a gradual acceptance of privacy principles. It is perhaps worth considering strengthening those enforcements. Fifthly, as we have mentioned, there are some questions about the growing use of electronic information and what we mean by 'personhood' in that respect. Sixthly, we have suggested, consistent with recommendations from earlier House of Representatives and Senate committees of inquiry into privacy, that the employment exemption should no longer be sustained. Finally, we suspect that the committee will hear a number of submissions from researchers about the growing enthusiasm for data linkage, not simply of health records within HealthConnect, but of a variety of other research collections. That obviously has very many benefits but, as with most cases of privacy, there are public concerns and it is about how we can move that forward.

CHAIR—Dr Nicol, would you like to add anything at this stage?

Dr Nicol—Professor Chalmers has covered the key points that we both want to make. Certainly, I can talk to the particular issues of enforcement and notions of electronic collection of data.

CHAIR—In respect of the first point you made—that is, the need to integrate what I read as being state and Commonwealth legislation—what is the mischief that we seek to redress? What areas are not covered because of what you perceive to be a lack of integration or harmonisation?

Prof. Chalmers—The federal legislation considerably extended the coverage, particularly once the privacy sector regulations were brought in in 2000. But if there is an absence of state legislation, there are still major instrumentalities like universities and state hospitals that are not covered. Those gaps are obviously being filled largely with legislation. In New South Wales there is now the Health Records and Information Privacy Act and in Victoria there is the Health Records Act, but they are not uniform. For example, Tasmania, as you will be aware, has drafted some personal privacy legislation that has not been promoted or introduced as yet.

Dr Nicol—Could I correct Professor Chalmers on that point. It has been passed by both Tasmanian houses but it has not yet entered into force.

Prof. Chalmers—Thank you. I think that is the need. Within those acts there is the idea of national information privacy principles. There are differences between them which I think tend to make it an overly complex area.

CHAIR—Is inconsistency within the act and between the public and private sectors your major concern?

Prof. Chalmers—Yes.

Senator STOTT DESPOJA—Thank you for your submission and for once again putting the issue of health privacy generally and genetic privacy specifically before the committee. In your submission you support—and I recognise the timing of your submission—the establishment of, as the ALRC recommends, a human genetics commission. As you may be aware, the budget papers have provided for the establishment of and funding for a human genetics advisory committee. Do you have any views on that? I am not sure if you are aware of its announcement.

Prof. Chalmers—Yes, I am quite well aware. When we made our submissions to the Australian Law Reform Commission and the AHEC we supported the idea of the introduction of a commission. I think, broadly, that is a very sensible way of proceeding. There are clearly some matters which will not be fully classified as research or health, but my understanding is that the principal committee of the NHMRC will have—as it had when I was Chair of the Australian Health Ethics Committee—the capacity to speak outside of strictly health, because the NHMRC Act will allow a full coverage of the issues. So I think that is a very good step forward.

Senator STOTT DESPOJA—Indeed.

Dr Nicol—I realise that this is not part of the committee's reference but the subsequent ALRC inquiry into genes and ingenuity also gave certain roles to the human genetics commission in

relation to patenting. I think that is going to be a very important role for that organisation as well.

Senator STOTT DESPOJA—I have no doubt that this is something that this and other committees will be dealing with soon, but I do not want to spook my colleagues with more work in this area.

Prof. Chalmers—Without the introduction of the original genetic discrimination legislation in the Senate—I think you know that legislation very intimately—I am not sure that this country would have moved quite so quickly towards the establishment of the ALRC recommendations. I think it has spurred our attention.

Senator STOTT DESPOJA—Thank you. Having said that, I do note your earlier comments about preferring integration or changes to the Privacy Act as opposed to stand-alone legislation. I understand and respect that. I have said many times that the aim of that private member's bill was to get this debate moving. But I was curious to hear your comment, Professor Chalmers, about moving towards a possible health privacy act. Is that something that we should be considering or is that something that you really believe is some way off? I just thought that was an interesting point.

Prof. Chalmers—The interesting thing is that two of our most popular states have eventually reached a decision in the area of health and the way in which you organise health records. Knowing that we are now moving towards HealthConnect, the idea of keeping that entirely within the framework of privacy legislation, which in 1988 was principally directed in the Commonwealth towards records held by banks and our concerns of government records, I think that is a very strong separation which has developed. No doubt the committee will be getting some evidence from the state governments of both New South Wales and Victoria on why they felt there was something unique about health records—the way in which health records still tend to be held with health professionals and within our health services where, thankfully, we still have an ethos of public responsibility and public statutory duties towards the protection of those records.

I also think that the real material difference is that at times we do need to have a system of national access to those records for health epidemiological protection reasons. I am sorry I am going on a little bit, but I remember, when I was Chair of the Australian Health Ethics Committee, often having discussions with the Privacy Commissioner. His perception in those days was always that you try to get rid of records eventually, and that is the greatest protection. That is the fundamental difference. The health record will never be destroyed. You want to keep this in perpetuity because it informs our health system. And, because of that, I think there can be differences between our commercial records, our security records, our government records and the health records—that is why I want to make a couple of comments about data linkage later.

Senator STOTT DESPOJA—On that issue of genetic privacy, there are a number of submissions, including yours and, of course, that weighty tome, the ALRC-AHEC report, which make it clear that genetic privacy is not specifically protected in federal law, certainly, or arguably in state law either, although we did hear evidence about the Northern Territory and now perhaps Tasmania. What are the implications in today's society of not protecting genetic privacy or genetic information? You refer in your submission to the issue of genetic discrimination. The

four of you responsible for this submission know better than anyone the issue of discrimination involving genetics. Would you put on record if you are aware of cases of genetic discrimination or abuse of genetic privacy in Australia?

Prof. Chalmers—Yes. On behalf of Professor Margaret Otlowski I apologise for her non-attendance. Unfortunately she is in hospital with an illness. She would have been speaking to the two matters of discrimination and the employment exemption. She has been funded by the Australian Research Council for the Genetic Discrimination Project, or GDP. I would prefer not to give the number without checking, but I think so far she has identified about 24 or 25 genuine cases where genetic information has been used in a discriminatory fashion. That project has not concluded. That is not to say, however, in the interpretation of that, that these are simply a few single instances. I think it shows that it has the capacity to be used in that fashion. It is a protection, therefore, that I think should be introduced to ensure that in the future it is not used against the interests of individuals.

I think the second thing she would say is that the capacity for information about genetics to be gathered is now increasing evermore and, unless we put in the framework now, there is a real potential for it to be used. She would also say that we should be conscious that some of the very serious concerns about genetic discrimination emanated from a very different situation that applies in the United States with their health system. Finally, she would have wished to have recorded that she would like to see that employment exemption removed in the privacy legislation.

Dr Nicol—I would like to add one comment. We would not submit that genetic information is not covered at all by privacy legislation. Certainly, in most cases, it would fit within the definition of health information within the privacy legislation and the way that the Privacy Commissioner has made determinations about health information. However, we do see that there are certain additional factors that need to be considered in relation to genetic information. We certainly support the recommendation of the Australian Law Reform Commission to extend the definition of personal information to include not only the information that comes from genetic samples but the genetic samples themselves.

Senator STOTT DESPOJA—Your submission makes very clear the specific nature of genetic information or how it is different from general health information. I am just looking at page 4 of your submission, where you talk about its familial nature, its highly personal and sensitive quality, its probabilistic aspect and the predictive nature et cetera and I am very keen to establish that difference.

Professor Chalmers, I acknowledge your comments about the distinction between the system that operates in the United States and the system here, and thus the different requirements in legislation that deals with privacy or, more specifically, discrimination. I acknowledge that my bill was based very much on the US experience. Thank you for your contribution.

Senator MASON—Professor Chalmers, I have a question that relates to Senator Stott Despoja's line of questioning. Does the current legislation inhibit medical research?

Prof. Chalmers—I would hope that it did not. Certainly in my time with the Australian Health Ethics Committee—and I note that you will be talking to Dr Kerry Breen, the current

chair, and to Professor Colin Thomson—we were at great pains, when we drew up our national statement, to ensure that we included for the very first time in any statement around the world a whole series of directions for ethical and responsible genetic research. We would hope that that has facilitated the introduction of very high standards. But you will probably find that, with regard to privacy as a whole, rather than any rules about genetics, those two witnesses will say that, yes, there are still some grumbles within the research community about the whole ethics review—that it sometimes takes too much time and that privacy issues can sometimes be quite complex and tricky, particularly relating to sections 95 and 95A, which are the reporting sections in the current privacy legislation. If you wish, you could cover those questions with Dr Breen and Professor Thomson.

Senator MASON—On page 5 of your submission, you say:

… enforcement mechanisms contained within the Privacy Act … are relatively weak.

You explain why they are weak. What should the committee do? What do you recommend to solve this mischief?

Dr Nicol—Certainly, at the moment, determinations of the commissioner are not binding on either of the parties. So it is then up to the commissioner or the complainant to bring a further action to the Federal Court and there is another hearing de novo, so it is a fairly lengthy process to get anything in the form of enforceable requirements. One area that might be instructive is schedule 5 of the Broadcasting Services Act relating to censorship of the internet. The provisions in schedule 5 relate to determinations of the Australian Broadcasting Authority. They define them as online provider rules, and those rules are binding such that, if the rules are not followed, it becomes an offence, so it is an offence not to follow the determinations of the Australian Broadcasting Authority. Perhaps a similar procedure could be put in place for the Privacy Commissioner so as to give the determinations of the Privacy Commissioner some binding force.

Senator MASON—Do you have anything to add, Professor?

Prof. Chalmers—No, that is our view, as expressed in the submission.

CHAIR—Thank you both very much for your submission and your evidence this morning.

[9.48 am]

BURTON, Ms Pamela, Legal Counsel, Australian Medical Association

NESBITT, Ms Julia Margaret, Director, General Practice and E-Health, Australian Medical Association

CHAIR—Welcome. You have lodged submission No. 9 with the committee. Does it need to be amended or altered, or would you like to start off with an opening statement?

Ms Burton—Our submission, you will appreciate, is confined to the effectiveness and appropriateness of the Privacy Act as it applies to the health sector so we have addressed only some of the terms of reference. From the outset the health sector has faced some difficulties applying generic principles—the national privacy principles—to health-specific situations. The matters that we would like to highlight are the concept of 'primary purpose' in NPP 2; the difficulties with the access principle that medical practitioners have; security of electronic records—about which we would like to mention some recent events to illustrate government and commercial insensitivity to patients' privacy concerns; and the national consistency, or inconsistency, of privacy laws and our fears of flaws being repeated in any overarching health privacy code.

In relation to the generic privacy principle, particularly NPP 2, we have highlighted potential interference with delivery of quality health care arising out of the narrow statutory concept of primary purpose that restricts a commonsense use of health information in the delivery of health services. It tends to dictate an episodic approach to health care. One unintended consequence was dealt with by a public interest determination that exempted consent compliance to permit the taking of comprehensive medical and family histories. Medical practice as we know it would have come to a halt. It illustrates that the one-size generic privacy just does not fit all.

We have urged over the last four years that this NPP 2 should be construed broadly enough to permit a holistic approach to health care. Proactive and preventative holistic care is quality care, and episodic care can be unsafe. Privacy principles were never meant to dictate clinical practice. Of course, patients can and do opt out if they want a health provider to simply deal with the proverbial cut finger and not have their medical records delved into, which may be appropriate to ascertain whether a history of epilepsy or domestic violence may account for an injury. Patients have always had that option, and still do. We have said in our submission that privacy legislation dealing with the way health records are to be handled should not dictate the nature of clinical care.

We understood that the Office of the Federal Privacy Commissioner had legal advice that NPP 2 was not open to such an interpretation. We have had to work with this. The current privacy commissioner appreciates the dilemma that the generic nature of the privacy principle has caused health professionals; however, in her review recommendations, which were released on Wednesday this week, she has not recommended amending the principles. Instead, she takes the view that this principle can after all be interpreted to accommodate a holistic approach in the medical arena. A different commissioner brings a different view. We will have to wait to see

whether this can be done satisfactorily or not. We would prefer some certainty in the legislation on that issue.

Our other major concern was around the access provisions. The right to a doctor's thoughts and notes has potential to interfere with the therapeutic relationship, particularly in the area of mental health care. Our submission has been that the legislation needed to be amended to lower that threshold to permit withholding access where harm might be occasioned to a patient. That problem was also acknowledged by the current federal Privacy Commissioner in her recent review recommendations. Again, she sees no need to amend the NPPs and does not recommend that. Rather, she sees that this can be resolved by developing appropriate guidelines. As I read it, this would require deeming an interference with the therapeutic relationship to be a serious threat to life or health, where harm might occur. Again, with a different privacy commissioner comes a different view. In our submission we say this is not a satisfactory approach to effective privacy law. It would be better for the legislation to be amended and clarified accordingly. That may be done by an overarching health privacy code. I will come to that when talking about the consistency of privacy legislation.

On the issue of electronic privacy: again, over the last five years we have urged that proper privacy controls over the security of electronic records be put in place. This takes resources to keep up with technological changes, and we would submit that further resources are required by the Office of the Federal Privacy Commissioner to meet this demand. The AMA put in a separate submission on the MBS and PBS privacy guidelines in which we urged that the current protection under the privacy guidelines on the MBS and PBS should be at least maintained if not increased. One of our biggest concerns as we go into electronic health issues is the need to protect against data linkage and to ensure that patients have full knowledge about it and know what they are consenting to.

While on this point I would like to refer to two current situations that have caused the AMA some concern. Recently we expressed concerns over the activities of a particular company known as HCN—their collection of de-identified patient data from medical practitioners. The federal Privacy Commissioner investigated and said the HCN's activities were okay because it was only dealing with de-identified information and that did not come under the privacy legislation. But that pays no attention to the dilemma that medical practitioners, who will find it difficult to comply with their privacy obligations, are placed in. Firstly, the information they are collecting from patients is not in de-identified form at that stage, and it does come within the Privacy Act. Doctors are obliged to inform their patients about how their information will be used and for what purposes. Patients need to know this so that they can question the de-identification process and its security, and some will object to their information, even in a de-identified form, being used for commercial gain. As we have ascertained, some doctors are unaware that the information can be used for commercial purposes. Unless they know what it is being used for, how can they properly inform their patients?

The other issue is the HIC's prescription hotline. This is a valuable tool for practitioners concerned about their patients' doctor- or drug-shopping. However, while the HIC can ensure that its activities in providing doctors with information about patients' prescription-shopping activities without their consent are lawful, it too did not consider the obligation on doctors before they are permitted to receive such information. This led to a last-minute flurry for the Privacy Commissioner to produce a public interest determination to exempt doctors from obtaining

consent in this situation. Again, the doctors' obligation to inform their patients, from whom they receive information, was ignored. It was ignored in that public interest determination. It simply stated that it was okay to do this under NPP 1.3, which requires you to tell patients where you collect information from.

The final matter we raise is the national consistency or inconsistency of privacy law. Our major concern about the privacy code of the Australian Health Ministers Advisory Council, AHMAC, is that to accommodate what I would call the current mishmash of state, territory and federal laws and private and public organisations the highest privacy standards have to be incorporated otherwise someone's law would be breached. Unless and until the generic national privacy principles are tailored to apply in a commonsense manner so as not to interfere with best clinical practice, we say that this code should not proceed to be used as a model for a binding code. In other words, the health privacy laws have to be sorted out first before trying to incorporate an overarching health specific code.

The fact that this AHMAC code is dealing with federal and state jurisdictions' privacy law means that it cannot be incorporated at the moment into the federal privacy law. It has not been explained how this is happening. As far as we are concerned, there has been totally inadequate—I could almost say no—consultation. There has been a little bit in the earlier stages. At present, it cannot be incorporated in the privacy law while it purports to bind state governments and their agencies. Having said that, I think everybody is in agreement that we really need a consistent, health-specific privacy law that covers all the jurisdictions and private, public and state organisations. They are the matters we have highlighted. Julia and I are very happy to answer any questions about the AMA submission.

CHAIR—You may have answered them already. In paragraph 5 on page 11 you talk about the federal Privacy Commissioner and the role that she does not have at the moment with respect to the health agenda. It is a structural deficiency, I think, you have identified. How important is that to you? The point starts:

Thirdly, the AMA is concerned that the Federal Privacy Commissioner is not represented ...

Ms Nesbitt—We do have some concerns that the Privacy Commissioner has not been involved in any of the major forums on electronic health issues. We think the issues are becoming very complex and that the input of the Privacy Commissioner would be incredibly valuable. The fact is that, while the development of electronic systems at a national level is clearly within the context of the Privacy Act, the question, really, is how to comply with the Privacy Act in an electronic environment. That is where we think the Privacy Commissioner's input would be very valuable.

CHAIR—Can you just elaborate on the concern about the Medicare smartcard and consumer ID number, and whether you actually think the smartcard can be controlled.

Ms Nesbitt—Whether the smartcard is the best technology to use for these purposes is a question that still has not been answered. I think that sort of research is going on. I know the National E-Health Transition Authority is advising the government on solutions. The smartcard was announced last year and has been introduced. It is a new Medicare card and contains a separate chip that contains a number. Our concern about that is that, while we are told that the

chip is not yet functional, there has still been no discussion on what the purpose of that chip is and what the purpose of that number is. It goes to the issue of the development of a unique patient identifier—the key to protection of an individual's privacy and their understanding of their rights under the Privacy Act. There must be a purpose associated with that number so the limits of the use of that number can be understood. That has not occurred in relation to the Privacy Act. We are concerned about the number. There was no consultation on the launch of the smartcard, either.

Senator MASON—We just heard some evidence from Professor Chalmers and Dr Nichol from the Centre for Law and Genetics at the universities of Tasmania and Melbourne. I asked them a question about medical research. I think their evidence was that the Privacy Act and the regime relating to medical research did not really inhibit, in practice, medical research. I note that in your submission you say it does. You believe that it is a narrow view taken under the NPPs when the research has to be relevant to public health or public safety. Could you expand on that and tell me why you think that is too narrow. As you know, medical records are very sensitive information. Publicly of course it creates all sorts of tension when records do not remain private.

Ms Burton—This submission was elaborated on in more detail in our very original submissions to the Privacy Commissioner in 2001 in relation to the guidelines that were being developed. The interpretation of the national privacy principle in relation to public health or public safety was very restrictive indeed. Again, I am not sure whether that is the way in which a particular privacy commissioner is construing it or whether it is open to some other interpretation and that in practice it is accommodating research. It was restricted to public health or public safety in relation to major issues like epidemics and water pollution and not individual research for, say, breast cancer.

Senator MASON—To be fair, Professor Chalmers did touch on that before. I do not want to mislead you about what he said. It did not generally inhibit but there are situations where it could.

Ms Burton—It could preclude. If you wanted more information on that we could come back to you with some more.

Senator MASON—I was going to ask you a question about the exemption of political organisations from the Privacy Act but I suspect Senator Stott Despoja will ask you about that.

Senator STOTT DESPOJA—With that opening, how can I resist? I am not going to ask a specific question about that. First of all, I commend you on your excellent submission and comments this morning. I note your comments about the political exemption and I accept them. But in the same submission you are arguing for a change to NPP 2 in relation to 'a serious threat to the life or health of any individual' et cetera so that the threshold is lowered. So you are arguing, potentially, for doctors and medical records to have a weaker threshold. I need you to convince me. In your opening comments I think you were referring to potential cases of domestic violence and others, and 'patient harm' was your preferred terminology. Why should we on the one hand criticise politicians for having an albeit ludicrous exemption in the act and on the other hand give doctors more power to withhold patient information or medical records? Why should we give you a lower threshold?

Ms Burton—I had not perceived any inconsistency. It is not a total exemption for politicians; it is a modified one. There is a total exemption for the media, I think.

Senator STOTT DESPOJA—We are pretty totally exempt.

Ms Burton—That is how it transpires. I do not think I have the example here but we were very concerned about what we saw as an abuse of that power in a particular situation where the power was not being used because of possible public harm or public interest but for a purely political advantage that involved a religious or some other political philosophy. We do not ask for doctors or medical practitioners to be totally exempt either. We are saying that the privacy and records should be enhancing clinical practice and that the threshold can interfere with clinical independence and good clinical practice.

I think you have raised the issue of having generic principles that do not really take into account the specifics of a particular industry—and the medical profession is a very good example because it directly relates to the health of people. They are interested in the health of their patients, and medical records are used more by medical practitioners than politicians. So we raised that exemption, together with the media exemption, because of the particular instance where there was no control and because of the power that politicians have to ring up an agency and reveal or disclose information without any checks or balances. At least the medical profession have all sorts of checks and balances and codes of conduct and so on. That is the best I can do without notice.

Senator STOTT DESPOJA—I can see the difference. You are arguing that there are rules that apply to the medical profession and medical records. In our case, as politicians, there are no rules—we are exempt. I am not defending that exemption because I think it is wrong. However, I do see distinctions. When people come to one of us they might come with sensitive personal information, but I would argue that there is nothing as sensitive as the kind of personal, health or genetic information that is confided to a doctor by a patient in that doctor-patient relationship. In your submission you very clearly argue for amendments. You claim they are required:

... so that the inappropriate threshold of posing 'a serious threat to the life or health of any individual'—

and that threshold is at 2.1(e)(i) of the National Privacy Principles—

is lowered so that patient information can be withheld where access could cause patient harm or interfere with a treatment protocol.

You are arguing that the language in that principle should be changed to 'harm', presumably—

Ms Burton—This is for access.

Senator STOTT DESPOJA—Yes, but I am trying to work out what that threshold is. I am happy with the threshold as it currently stands. I have heard some of the examples you have given as to why it should be changed. But the examples that you have given me strike me as exceptions to the rule and not a good case for changing that principle to lower the threshold. You say:

There are occasions where access to clinical notes can cause harm to the patient or interfere with the therapeutic relationship. This poses a serious problem for doctors ... fails to protect the doctor's private or preliminary views ...

We have heard these arguments before. I am not convinced by them in toto. I want to know why you would weaken the threshold for doctors in this instance as opposed to having it in exceptional cases and leaving that to the Privacy Commissioner or someone else to determine. Why do doctors need a lower threshold?

Ms Burton—In particular, it is for those medical practitioners and health service providers involved in mental health care. That is where it has been raised over and over again, for two reasons. Firstly, as to the harm—it is not and/or—interfering with a therapeutic relationship can be harmful. The Privacy Commissioner agrees that it could cause serious and imminent harm. But it can be harmful simply because in that particular relationship there is an interaction of thoughts and ideas between the provider and the patient. Patients may demand or want to know what it is that the therapist is writing down when the therapist might only be having preliminary views, reacting or having their own thought processes and so on. That could cause the patient, at the minimum, to leave that person and find somebody else and so on. The continuity of care disappears at a very vulnerable stage for the patient.

Secondly, interlinked with that is something that we, as lay people and not doctors, did not understand—and we worked very closely with doctors and Malcolm Crompton, the Privacy Commissioner, and discovered this—that mental health therapists or clinicians are putting themselves in their notes as well. There is this interactive relationship. They might in fact be writing down things that they would not want to see the light of day because they could change their minds next time. It is an evolving relationship. They are trying to find out what is going on with a person who might be in a vulnerable mental health state.

There was so much talk of having two separate sets of notes—that is, (1) their own personal thoughts and feelings and (2) recording information about a patient. But they do not have two sets of notes; they just write as they go. There was discussion about how this can be blacked out or sorted out. Of course, a patient receiving a set of notes with blacked-out words raises more questions than it answers. So this became a subject. Malcolm Crompton took this very seriously and set up a group. He worked with the Mental Health Council of Australia, carers, patients and the AMA—all sorts of hospitals and groups. We worked together to try and work through this under that existing principle that you have referred to without lowering any thresholds so that their work could go on in the way it should go on and so that they would not have to change their practices.

This privacy legislation is not meant to tell doctors how to act clinically. It was threatening psychiatrists and general practitioners, saying that they would have to no longer take these notes and do this interacting and so on. We thought, 'Really, the clinician should decide if this is harmful.' That is not to say they should not abide by the privacy rules wherever they can, because it enhances and helps. It would mostly help patients. There is no suggestion that we want to resist providing patients with information they are entitled to know and need to know, but there is some clinical judgment needed here. To say, 'It's definitely not life threatening, but this could cause harm,' is, in a clinician's mind, a very dangerous situation—it would have to be life threatening before they could withhold access to those notes. It is a dilemma.

Senator STOTT DESPOJA—I think it is. I take on board your point about 'serious threat to the life', but the current provision also allows for 'serious threat to the health'. As a citizen, I feel somewhat protected by having the word 'serious' in that statement. That gives me some security as a citizen—I kind of like that buffer.

Ms Burton—As a patient, though? When you might be—

Senator STOTT DESPOJA—You bet, because I believe that, as a patient in exceptional circumstances—that is, where my life or my health is seriously threatened or affected—this sufficiently covers that. I am not sure I necessarily believe, if it were changed and watered down to 'harm', that that would be strong enough as an argument either for someone to access those records or, in the case of NPP 6, which is also part of this, for me not to have access to or the ability to correct my own records. So I take on board your point because I recognise there are exceptions, but we are now talking about changing that. This will be a watershed once you change this. It does not just apply in exceptional circumstances—you would hope that it would only apply in exceptional circumstances but it does not have to. That is not meant to be a reflection on the medical profession; it is a reflection on views on privacy. Please do not get me wrong, because, as a politician and not specifically as a patient, I recognise we have an exemption, which I think is inappropriate. But I think you have access to much more extraordinary information.

CHAIR—I think you need to get to a question, Senator Stott Despoja.

Senator STOTT DESPOJA—I am just clarifying for the record that you are talking about changing 'poses a serious threat to the life or health of any individual' to 'harm—

Ms Burton—It is in the provision for access that is NPP 6. It is not 'harm' generically at all but harm in this medical practice situation. I can absolutely understand what you are saying, but we have heard some horrific examples. For instance, there was a psychotherapist who was seeing a very disturbed patient in the early days and, not knowing the causes, queried abuse as a child—maybe sexual abuse; question, question—and then, as the therapy progressed, eliminated those thoughts and had others et cetera.

In one case there was great success, and the person five, six or seven years later was doing very well indeed. They were stable and living a normal life. They asked for access to these notes. These are very interactive notes of the psychotherapist about their own feelings. The notes were made available, as one would expect, particularly as the patient was possibly vulnerable but certainly improved. The patient, reading that sexual abuse and some other details I cannot remember had been thought about as possibilities, went into a steep decline. It was a dreadful situation. Those stories have come up over and over again. That was one where it was remote, years later. But you can imagine what would happen if it were at the same time.

I understand what you are saying, but it might be that this has to be devised and thought about very carefully. It is driving—there is no question about this—those therapists into different practices. They will not put down their intimate thoughts about their reactions to the patient, like 'this patient feels hostile'. This is what they do. GPs, in treating a broken leg, do not. They would not need to; it is not relevant to the therapeutic process. But in treating a vulnerable or mentally unstable patient, yes. If they are doing that interactive process they will record their

own thoughts and feelings. Possibly they believe the patient has been dependent on them or is making advances to them. This will not now be recorded. If someone takes over that therapeutic process or the person comes back five years later, it is very difficult for practitioners. Maybe we need some really deep understanding from both sides who have thought about this on the assumption that the clinicians want to do what is best for their patients. If we make assumptions that they are not, we get this wrong. We have to assume good practice and deal with bad practice in a different manner.

Senator STOTT DESPOJA—I accept that. I think you are right. It is not the argument that I am contending. It is just a matter of what the solution is—whether it is making a change to that NPP 6 or, as you say, further debate and discussion. I know, Acting Chair, I have taken up too much time. Can I put a couple of things on notice?

ACTING CHAIR (Senator Payne)—As long as Ms Burton and Ms Nesbitt are comfortable to take those on notice.

Senator STOTT DESPOJA—You have heard this morning, and you mentioned it, about the idea of a human health act, a health privacy act or some kind of stand-alone legislation. I would be really curious to hear if you would be willing to elaborate on that in a question on notice.

Ms Burton—I was actually referring to AHMAC's idea of the overarching health privacy code. The Privacy Commissioner, in her recommendations that have just come out, talks about incorporating that code as some kind of binding schedule to the federal act. It is talked about. Legally it is not possible at the moment unless all states cooperate and give that power across. The AMA have, right from the outset, always said we would like an overarching health specific privacy code. While we are really in favour of the privacy principles, including the access and the patient rights, we were disappointed to see such a generic provision for privacy when the states were separately dealing with health specific records legislation quite separately. They are in conflict.

Senator STOTT DESPOJA—That answers my question. I will not ask you to answer this now, but will you take this on notice: are current privacy laws sufficient in relation to newborn screening and testings, specifically Guthrie cards? I am just wondering what the AMA's view is on current consent and privacy provisions in relation to Guthrie cards, newborn screening cards or whatever you call them, depending on what state you are in.

Senator LUDWIG—You mentioned the de-identified information that was being collected. What was the purpose of that? What was it being collected for?

Ms Burton—I might let Ms Nesbitt answer that. This is the HCN. Indeed we were trying to find out. The purposes stated seemed not to be clear at all.

Senator LUDWIG—I imagine it was for marketing.

Ms Nesbitt—The doctors joined what was called the General Practice Research Network. By joining this network they received an additional piece of software for their computers. The brochures say that the patients' information will be used for all sorts of research. Some of the brochures do mention that it might go to pharmaceutical companies, but it is not made clear how

it will be used. It is not made clear that it is for commercial purposes. Certainly, our overriding impression was that a lot of the correspondence we received was to do with the fact that data would be sent to educational institutions for research. Our issue is clarity of purpose. GPs should inform their patients about what this data is being used for and provide patients with the opportunity to opt out.

Senator LUDWIG—Does it breach any privacy principles as you see it?

Ms Nesbitt—As Pamela has indicated, we have some concerns about the findings from the Privacy Commissioner on this matter. From my perspective, particularly in relation to issues of electronic health records, the interpretation puts the doctor in the very difficult position of being unable to inform a patient of the purpose of the use of de-identified data. It also puts them in conflict with their NPP 1 obligations to inform patients of all uses of the information they are collecting. The other issue is that in some senses the finding seems to indicate that the patients' right to opt out is lost. If there is no need to inform the patient of the use of their de-identified data then their right to opt out no longer exists.

Senator LUDWIG—So it is embedded software. The doctor does not have the ability to switch a flag on or off to indicate whether information is being collected, because it is input data from the doctor about the types of prescriptions, injuries or diseases.

Ms Burton—They can switch it off if the patient says no. However, we understand that there have been problems with all the data being sent and the collector then saying, 'We've now got this flag saying this one should not be included, so we will send it back.' There is that complication as well. But our concern, which Julia has raised, is the difficulty the doctor has in telling the patient, when they are collecting the identifiable information, what all the purposes are so that the patient knows what they are not opting out of. While research is understood and a lot of medical practices have in their privacy policy the line 'some of your information may be used for research', as soon as there is a mention of it possibly being used for commercial gain, we have seen the reaction of both doctors and patients who did not know this. They say, 'Why should anybody be making money out of my information, de-identified or not?' It is something that should be up front, that they should be told about. They should have a right to opt out.

Senator LUDWIG—The second issue is in relation to the Medicare smartcard, if we can call it that, which is being trialled in Tasmania at the moment. You said that you were not consulted about it. Have you since been consulted about the operation of it?

Ms Nesbitt—I think we were consulted after its release. So I would say, no, we were not consulted. We discussed it.

Senator LUDWIG—Has more information been provided to you since then?

Ms Nesbitt—No, and, in fact, some of the forums where we would have obtained that information in the past no longer existed at the time. The MediConnect development group, the HealthConnect advisory group and all those forums where these sorts of things would normally be discussed no longer existed once the announcement was made.

Senator LUDWIG—What is your view of that? Are you dissatisfied at not being consulted on the operation of the card, given that it will be swiped at doctors' surgeries and the like?

Ms Nesbitt—We were very concerned.

Senator LUDWIG—Have you expressed that?

Ms Nesbitt—Yes, we have, very strongly. And that is why we received a visit from the Health Insurance Commission; they gave us a briefing on what was happening. Our main concern was about the incorporation of the chip and the inclusion of a number—the function of which is still unclear.

Senator LUDWIG—Has the range of data that is going to be kept on the card been indicated to you?

Ms Nesbitt—No. We have indicated that we want strong consultation should the smartcard be the solution that the government ultimately accepts. We want strong consultation about what should be on that card. They were talking about all sorts of things being on the card—for instance, allergies. It is not good clinical practice for a patient to go into Medicare and say, 'I'm allergic to this and allergic to that.' It needs really close consultation with the medical profession about what should be on it. What is the most important information, what is really necessary, from a clinical perspective, should be on the card. The other issue about what is included on that card is to understand what the purpose of that information is. There is the opportunity to obviously put a great deal of information on that chip that may not be related to clinical purposes, and therein lie issues of data linkage.

Senator LUDWIG—The second issue that arises from that, whether or not you have considered it, is that—and at this point in time we will confine it to medical information that is relevant to the patient which is put on the Medicare card and then carried about—if you go to one doctor and they swipe the card, do they collect the information at that point? And, following my scenario through, if you then go to another doctor who is unrelated to the first, and the first doctor sees you about X and you see the second doctor about Y, in the normal course of events that would be discrete data held by one doctor and discrete data held by the other. Doctor A and doctor B—and we confuse it with more alphabet—do not have an automatic right to share that information. In this instance, if you have gone to doctor A and then taken your Medicare card and gone to doctor B, doctor B picks up all the records from doctor A, if they have been updated on that card.

Ms Nesbitt—We cannot answer that question as yet. The smartcard is one of the options in the development of a capability to share clinical records. I am not sure how that would actually be done in the future. If the smartcard were the way to go, and we agreed to a sharing of records through that card or that card gave access to doctors, that would be the way they would do it. A lot of questions are still to be answered even around the issue of shared electronic records and the level of consent—for example, should patients be able to mask specific things on their records? All those questions are still being discussed and need to be discussed to find the ultimate solution. You are correct in that, ultimately, the goal is to find a means for clinicians to be able to share patient information, including treatment received from other practitioners.

Senator LUDWIG—So the AMA's view is that the sharing of data between doctors and clinicians is permissible or a goal—in other words, to have a seamless web?

Ms Nesbitt—The capacity—

Senator LUDWIG—I am not sure that I agree with that, because as a private patient you may want to separate your doctors, depending on the type of treatment you are receiving.

Ms Nesbitt—They are exactly the issues—those in terms of consent—that we are grappling with within an electronic environment: what levels or limits can patients put on access? They are things that we have been and are still grappling with. Decisions on how that will occur will have to be taken on the basis of the eventual solution that is developed.

ACTING CHAIR—Ms Burton and Ms Nesbitt, thank you both very much for appearing before the committee and for your submission. You have taken some questions on notice, and we will be provided with those through the committee secretariat. We look forward to receiving those answers.

Ms Nesbitt—Thank you very much.

[10.35 am]

CLUTTON, Mrs Cathy, Acting Executive Director, Centre for Health Advice, Policy and Ethics, National Health and Medical Research Council

HILL, Professor David, Member, National Health and Medical Research Council Research Committee, and Chair, National Health and Medical Research Council Working Committee on Privacy, National Health and Medical Research Council

THOMSON, Professor Colin John Houston, Consultant in Health Ethics, National Health and Medical Research Council

WHITEMAN, Dr David Carlisle, Council Member, and Member, National Health and Medical Research Council Working Committee on Privacy, National Health and Medical Research Council

ACTING CHAIR—Good morning. The National Health and Medical Research Council has lodged a submission with the committee, which we have numbered 20. Do you wish to alter or amend that submission?

Prof. Hill—No.

ACTING CHAIR—I invite you to make an opening statement, at the conclusion of which we will proceed to questions.

Prof. Hill—Thank you for the opportunity to speak to our submission. The NHMRC have an interest in any matter which impinges on the health of Australians, in particular from a population-wide perspective. The NHMRC got involved in the issue of privacy law and regulations impact on health because of a growing number of anecdotes and stories we were hearing from clinicians about difficulties that were arising, in their view, in carrying out their work as well as they could and from researchers finding obstacles to being able to do effective research. We wanted to find out whether these stories were real, whether they were exaggerated, whether it was because doctors and researchers did not really understand what the regimes were or were not applying them well, and whether managers or data custodians were manipulating privacy law in some way for their own ulterior purposes.

We decided to do a comprehensive investigation in two parts—a legal analysis and an empirical study of individuals and groups that seemed to have a stake in the privacy issue. We wanted to do this to see whether there was real substance to the concerns that we were hearing raised in the medical and research communities. We found in terms of the legal analysis—and Professor Thomson could elaborate on this—a couple of top-line findings. I think you have heard about this. There is a patchwork of privacy regulation around the country which is confusing and difficult to work with, and there are some problems with sections 95 and 95A. In the empirical studies we collected a large amount of information on the opinions and experiences of the stakeholders concerning the impact of privacy. We included a number of groups as stakeholders—the general public, health consumers, people who had high usage rates of the

health system, practitioners, data custodians, peak bodies and medical researchers. In a moment, Dr Whiteman will outline some of the key features of the surveys, because I think senators have raised a number of questions about the level of public concern and the perception around some of these issues. We have some data on that.

I want to address why researchers want to be able to conduct data linkage studies without the express consent of every single person whose data is involved. We do not believe any study involving data linkage should be undertaken without a properly constituted ethics committee considering and approving the study and having concluded that the public interest outweighs any loss of privacy for individuals and that there is adequate provision made for confidentiality of information where personal data is used. When such work is done, researchers work with deidentified data. There is no intrinsic interest in the personal identity of a person once one is sure that we are talking about the same person from two or more different databases. This of course excludes the possibility of inadvertent or mischievous disclosure when you are dealing with the data at that level.

I would like to clarify why researchers need to have personal identity to link data sets. Firstly, it may be impractical to get consent, simply because of the sheer cost of doing so. The sorts of studies envisaged by epidemiologists and public health researchers usually involve tens of thousands in some cases and imaginably millions of individuals. At that level it is impractical. Secondly, related to that of course is the logistics: how could you make contact with people?

The most important reason why it is necessary to have personal identifiers to link data sets is that, if not everybody can be contacted to obtain individual consent, selection bias might arise. Selection bias seriously challenges the scientific validity of any findings. It occurs when the people who are contacted and give consent to be included differ in some systematic way from those who are not able to be contacted and therefore consent. Recently we had publicity about the drug Vioxx and its harmful effects down the track which were not discovered obviously when the drug was first approved for use. We know from experience in other areas that it would be highly likely that those who had been prescribed Vioxx and/or had a heart attack would be more likely to be accessible for contact because they are in the health system and more likely to agree to participate in the study. You can see that by systematically including those one could easily come to a false conclusion about the relationship.

Sometimes obtaining consent can lead to the creation of avoidable alarm in people contacted. That does I admit sound like a rather patronising position to argue but if you can imagine the case of a person who had been treated with a certain drug in childhood and a hypothesis arose that that treatment might have adverse effects down the track that could perhaps be related to cancer, one would be asking people, with very little evidence yet of a real effect, to have their data on their earlier treatment linked with the cancer registry. This can put people in a position of fairly helpless anxiety in the intermediate period. That is the third reason why—and a rare one possibly—an ethics committee might consider agreeing with a study for data linkage without individual consent. Dr Whiteman can now talk about the survey data.

Dr Whiteman—I think the summary of the surveys was tabled with the documents, and there are some charts here. There are two comments that I would make in relation to the discussions today. Firstly, around the attitudes of the general public to linkage of health databases with sensitive health information, we found it really does depend on how the questions are phrased.

When people are just given cold the question of whether they would like health data matched, about 66 per cent of people in the general community either strongly approved or approved of that activity—so more than half. When people were asked whether data linkage of health information would be permissible if there were unique numbers and no other identifiers involved—if it did not involve names—then the rate of approval went up to 82 per cent in our nationally constituted sample. Those are quite interesting figures to us.

CHAIR—I wonder, just on that point, if you could have that information made available for us.

Dr Whiteman—Yes, those details are available, and the full report is available on the NHMRC web site and was part of the submission.

Senator MASON—Including the questions you asked and so forth?

Dr Whiteman—Yes.

Senator STOTT DESPOJA—Where is that 80 per cent figure?

Dr Whiteman—It is on page 8—these are double-sided pages—the top figure, 'attitudes to data linkage consumers'. Question 14 was: 'Could you tell me whether you think it is acceptable or unacceptable for approved researchers'—this is after they have had ethics approval—'to access information from databases where records are identified by a unique number rather than a name?' The general public is the left-hand set of boxes and the high-use health consumers were the right-hand set of boxes. This was a series of questions asked; we are taking a snapshot at the end of a range of questions.

The other point is in relation to the survey conducted of medical researchers and their feelings of change since the advent of the Privacy Act. This is recorded on page 4 of the handout. The bottom figure there shows that 25 per cent of researchers reported that research projects had either stopped or could not be started because of changes. About a third of the researchers reported that the scientific rigour of their studies had been compromised along the lines of Professor Hill's statement.

Senator MASON—Getting back to the issue raised by Professor Hill about the example of Vioxx—are you suggesting that if the Privacy Act were not constructed as it is, we in this country could have discovered earlier that there was a link between that drug and heart disease?

Prof. Hill—Yes. We are trying to convey to policy makers and the public generally that opportunity costs may exist because of barriers and difficulties that the privacy legislation puts in our way. Whilst privacy is an important value, we do not think the public or policy makers have made the connection between what is possible if we were able to link data sets more readily under proper ethical guidelines in this country. Vioxx is a very good example.

Senator MASON—It has received a lot of media coverage. There was something on TV the other day about how it was discovered in the United States, but it took a while to generate that sort of publicity in this country. You say New Zealand and Canadian privacy legislation are more relaxed and perhaps better. Why is that?

Prof. Hill—Can I ask Professor Thomson to comment on that; he is the expert.

Prof. Thomson—All three jurisdictions have a similar threshold test, which usually includes the words 'whether it is impracticable to gain consent'. Once that is satisfied, the Canadian and New Zealand systems then allow the use of identifying information without consent for research, provided that information in the course of that research will not be disclosed in a way that identifies any of the people. There is no other test. Australia has the impracticability of consent. New Zealand actually has an alternative: it says 'whether it is not desirable or impracticable'. I am not quite sure what that means, but that seems a softer or lower threshold. In Australia, the threshold of impracticability is there. Then, in addition, the guidelines require a discrete HREC—Human Research Ethics Committee—review, using a set of privacy considerations before and making the final determination as to whether in its opinion the public interest in that research substantially outweighs the public interest in protecting privacy. We add that as a necessary test. And even if the committee is of the view that the public interest in the research does so outweigh, the custodian of the data might still say, 'In my view, the privacy legislation precludes me from making that information available.'

Senator MASON—Senator Stott Despoja raised this issue before in her examination of witnesses from the AMA. I think all people are concerned about their health information, for all sorts of reasons. I have to say that particularly for people in public life, including politicians, the release of health information could be dire; in fact, it could really destroy someone's career. So make no mistake that we—as politicians and as ordinary citizens—feel that this sort of information has to be protected, nearly above all else. Have there been instances in recent history of confidential health information being released adversely to an individual's interests?

Prof. Hill—I am sure there have been, but we were racking our brains to think of a case where that happened in a research context.

Senator MASON—I am sorry; I mean in a research context, yes.

Prof. Hill—We could not think of any. As researchers, we of course quite appropriately feel very tightly constrained within the rules set by the ethics committee when the study is approved but, as I said before, usually, in terms of using the data around the labs and where it is being analysed, individual identification is of no value and is removed. We thought of that question and could not think of a case.

Senator MASON—You could quite literally destroy someone's career in public life.

Dr Whiteman—Certainly. It would be a severe disciplinary transgression for that to occur, and we are just not aware of that having happened in a research setting at all.

Senator STOTT DESPOJA—Welcome, and congratulations on a new committee. You have a genetics advisory committee as of the budget papers last Tuesday and $7.6 million to go with it over four years. Were you consulted, Professor, in relation to the establishment of this advisory committee?

Prof. Hill—No.

Senator STOTT DESPOJA—Do you have specific knowledge as to what the role of the committee will be? Will you get some role in determining the responsibilities of that committee?

Prof. Hill—Our working committee has actually finished its life, so in a sense we do not exist anymore. Dr Whiteman is on the council and may know more about this issue than I do.

Dr Whiteman—I am sorry; I cannot elaborate. I was out of the country last week and I am really only just catching up with this announcement.

Mrs Clutton—May I make a comment?

Senator STOTT DESPOJA—Absolutely.

Mrs Clutton—The committee has not yet been established but, as you say, it will be a principal committee of NHMRC, and it will be appointed by the minister following consultation with relevant stakeholders. It is anticipated that the principal committee will start its work to coincide with the beginning of the new triennium, which is January 2006. At the moment I do not have any more information than that.

Senator STOTT DESPOJA—Thank you for that. It is a welcome addition, but I might glean some more information from the department shortly. I will just go back to the issue of consent and so-called barriers in the way. I am the last person to want to put barriers in the way of scientific research, believe me, but I am also a bit of a fan of people being able to consent to use of the information. I ask Dr Whiteman, in particular: in response to the graph that you have been talking about, doesn't question 14 indicate that people are willing to have their information—whether it is personal information, DNA or whatever—used for the purposes of research, in this case with a unique number so it is essentially identifiable but still de-identified in the sense that it is not associated with a name? People are willing to do that, but they want perhaps to be consulted or to provide consent for that process. Is that really such a bad thing?

Dr Whiteman—It is getting the balance between the integrity of the research and the privacy of the individuals taking part in that study. As Professor Hill mentioned in his earlier address, once you go down the pathway for large samples—we are talking thousands or tens of thousands—and, for these large studies, you can only allow people into the study who have consented, they become a selected group of patients who may not represent the Australian population. Depending on the question that you are trying to answer, you may derive a false result that could actually do more harm than good. You may inadvertently find, in this selected group, that there is an association between drug X and disease adverse event Y that may not be real in the general population. It can cause alarm. The consequences are unknown but they are likely to be—

Senator STOTT DESPOJA—So you are arguing that you want to improve that initial sample for testing. Do you want to be able to do that through accessing information that has not been consented to be provided? Or are you talking about doing that halfway through because—as scientists have said through these graphs—due to privacy laws, if someone wants to provide consent for further testing and then pulls out, that compromises the integrity of the research? Are you talking about the initial sample or the hazards that go through the testing process?

Dr Whiteman—Both of those things. I would hasten to add that almost all of the research that public health researchers do involves consenting patients for their studies. But these are those special questions where you are using information that has been recorded in separate databases and you need to make that linkage occur. Usually, just the size and scale of those connections means that obtaining consent can be impracticable or not possible—for example, if the people have died. This happens when you are talking about historical or occupational cohorts where you are trying to follow up workers from a set of factories around Australia who were exposed in the 1950s to see what happened to them over time. Currently, that research is almost impossible to do in Australia, yet it was permissible up until a short time ago. These are quite profound changes in the way that knowledge can be gained and it can have a consequence of giving us the wrong answers if we insist upon consent for those sorts of data sets.

Senator STOTT DESPOJA—Okay. I feel a bit better about this now, because Professor Hill talked about barriers within the legislation. This is different from people who you do not think are going to provide consent; you are talking about the practicality of actually obtaining consent at all. That is an amendment that we could look at.

Dr Whiteman—The other thing to recall is that all of this is supervised by ethics committees.

Senator STOTT DESPOJA—Yes.

Dr Whiteman—It is not as if the research can happen in isolation; it still must go through the ethical review process. The difficulties lie in getting approval from ethics committees to undertake the research. It is variable because of different committees. Once approval has been given, as Professor Thomson has said, there is then no obligation at all for the data custodians to accede to that request for information. There are several barriers along the way because of perceptions about privacy as well.

Senator STOTT DESPOJA—Absolutely. In this day and age when you have some politicians scrutinising the work of certain ethics committees in relation to new technologies of course you do not want to go out on a limb. I understand better your claim to barriers within the legislation. At first I was wondering how much of this related to education. On page 8 of your key findings you talk about the researcher's attitude and looking at research that has either commenced or not commenced or been stopped as a consequence of privacy considerations. I am wondering how much of that really relates to people feeling more educated about or aware of their rights and actually not giving consent in the first place or stopping consent part way through. Maybe there is an onus also on researchers, scientists and doctors to make it very clear for what purposes—I know they are supposed to—that research is being used for. Thus, when I look at question 14, I get the impression that people are willing to provide that information but they need to know what it will be used for.

Prof. Hill—What would have happened would have been that those researchers would not have got started because an ethics committee interpreted the regulation in a way that made it very difficult for them. They would have said, 'You can do the study but only if you get informed consent from everyone.' They would have got started and then they would have found that biases were coming in and they would have lost heart in terms of finishing the study. That would be one scenario.

Senator STOTT DESPOJA—That is that almost distorted sample to which you referred; you do not have the right complexion.

Dr Whiteman—Yes, and that is a concern because in these kinds of studies you are trying to find the answer—the truth. If you know that you are on a path that is leading to a false conclusion, or you strongly suspect it, then as you are using public money you have some obligation not to pursue that. There is a balance there.

Senator STOTT DESPOJA—Thank you for that. Does the NHMRC have a view on or a role in monitoring the way that Guthrie card information or newborn screening samples are used for research? I am happy for you to take that on notice if you have any information to supply to the committee.

Mrs Clutton—We do not have a specific view but I am wondering if Professor Thomson can recall the detail in *Essentially yours*. There was some comment in there.

Senator STOTT DESPOJA—Indeed. I must admit that we have access to that. I was just wondering if there were a specific role or view.

Mrs Clutton—We do not have a separate opinion.

Senator STOTT DESPOJA—Thank you very much.

CHAIR—Thank you very much for your submission and your evidence.

[11.00 am]

LYONS, Ms Margaret, First Assistant Secretary, Health Services Improvement Branch, Department of Health and Ageing

McGRATH, Mr Mike, Legal Adviser, Department of Health and Ageing

MURNANE, Ms Mary, Deputy Secretary, Department of Health and Ageing

RICHARDS, Dr Brian, National Director, e-Health Implementation Group, Department of Health and Ageing

CHAIR—Welcome. You have lodged a submission with the committee, which we have numbered 34. Do you wish to alter or amend that submission, or would you like to make an opening statement?

Ms Murnane—We appreciate the opportunity to appear before the committee in relation to this inquiry into the Privacy Act. Our submission comprehensively covers a wide range of matters that the department considers important and wanted to bring to the attention of the committee. I will not go over them again in detail. However, there are a couple of issues that I would like to draw your attention to now, and there are a couple of new developments.

As the submission notes, the privacy of health information is an essential part of quality health care. It is accorded the highest value by consumers and health practitioners, and we acknowledge, respect and share that. We continue to support most strongly the need for specific protection for health information and the rights of individuals to have control over it. If people are not assured that their health information is adequately protected, they may not seek health care, which may then increase the risks to their own health and the health of others. Research is fundamental to quality health care. It benefits individuals, families and communities. It is important that it is able to be undertaken. However, the importance of the privacy of health information to an individual and the community generally is also of the utmost importance. We believe that these two imperatives can be reconciled.

In relation to HealthConnect, which we talked quite a lot about in our submission, we have recently introduced a revised implementation strategy for its delivery. We will be working in partnership with states and territories to ensure the implementation occurs successfully across Australia. The implementation will take into account local priorities, and we believe this sensitivity to local priorities will be able to be accommodated in the national framework. Most importantly, we plan for HealthConnect to be underpinned by Australian federal, state and territory privacy legislation. A working group has also been formed with states and territories to develop privacy and security rules and protocols specific to HealthConnect. Health care providers will be subject to strict privacy protocols as well as contractual obligations to prevent inappropriate disclosure of HealthConnect information.

I would like to say a little about genetic information. In the recent budget the government provided funds for the establishment of an expert advisory committee on human genetics. This

will be established as a principal committee of the National Health and Medical Research Council. Its role will be to provide advice on current and emerging issues in human genetics and related technologies, and to provide advice on the complex social, legal, ethical and scientific issues that arise from these technologies. The reconciliation of the privacy of an individual with imperatives of research and the benefits that will give to individuals' families and communities will, of course, be among these current and emerging issues that it will advise on. That is all I want to say at this stage.

CHAIR—Thank you. I will start the questioning. What information systems—the PBS, the health system or any other systems that contain personal information—has your department responsibility for?

Ms Murnane—The PBS and the MBS systems, and the aged care payment system does contain some personal information. The systems connected with the administration of vouchers for hearing aids under the hearing services act would also contain some personal information.

CHAIR—Do you keep a log of misuse, unauthorised use, abuse or hackers?

Ms Murnane—We do not.

CHAIR—You do not?

Ms Murnane—No. I will check that but, to my knowledge, those instances are rare. Dr Richards used to work in the HIC. Do you want to comment from that perspective?

Dr Richards—HIC maintains audit logs of access to all information, and any concerns about inappropriate access are followed up and, I believe, reported in the annual report.

CHAIR—Could you come back to us with, say, the last three years of stats on aspects of misuse, abuse, unauthorised use and hackers.

Dr Richards—We would need to obtain that information from HIC.

CHAIR—Is that for all the systems?

Ms Murnane—No. We can look at those other systems that I mentioned to you that contain some personal information, but it would not be as extensive as the HIC's. We will look at that for the last three years and come back to you with it.

CHAIR—Thank you.

Senator STOTT DESPOJA—I will begin with the HealthConnect card. The proposal came from Joe Hockey. It was mentioned in April that there should be some kind of link between that card and Centrelink. Is that happening and can you provide any more information on that proposal?

Ms Murnane—I am not aware of exactly what Minister Hockey said or the context. From the perspective of our department, at this stage there is no intention for the function of the

HealthConnect card to be wider than health information. Dr Richards, who is responsible for e-health in the department, might want to comment.

Senator STOTT DESPOJA—Dr Richards, are you aware of any discussions and information regarding the extension of this card or use of it with other government agencies?

Dr Richards—I have seen Minister Hockey's statements reported in the press, but there is no work going on the HealthConnect area of the department to link health information to other information.

CHAIR—So it has never been considered by the department?

Dr Richards—It is not under consideration by the department.

CHAIR—Nor has it been?

Dr Richards—Not that I am aware of.

Senator STOTT DESPOJA—In some earlier questions to other witnesses, I mentioned yesterday's comments by the Australian Privacy Foundation, which talked about the bear to the honey pot scenario: the idea that, when you start to concentrate or consolidate information in a particular place, that provides an increased incentive for people to hack into that system. Ms Murnane, I was interested in your comments in response to Senator Bolkus's question about hacking. Do you recognise or do you believe that increasing amounts of information in the one place, particularly in relation to this HealthConnect card, might actually provide a greater incentive for hackers or, if you are a consumer, a greater risk of your information being accessed in some way? What is the department doing about countering that with increased security measures?

Ms Murnane—It is hard to comment on what motivations of individuals and organised groups might be. Currently there is a lot of information about individuals held by the HIC and the record of safeguarding that has been so far a very strong one. As Dr Richards said, the HIC has a lot of internal controls, including audits of access, and anybody who uses inappropriately is immediately dealt with. It would just be an opinion, but we are alert to the agility and innovative capacities of hackers with all our systems. The security of the system would be paramount in building it.

Senator STOTT DESPOJA—Before Dr Richards responds, I want to add to this. I want to know specifically what security measures are being contemplated or will be implemented to protect that data. My understanding is that $128 million has been allocated to this project. Can you supply us with a breakdown of the privacy aspect and the security aspect? I am happy for you to take that on notice. It just seems a lot of money, in my opinion, has been allocated in recent budgets, particularly the last one, to potentially invasive schemes that deal with the privacy of Australians. I do not see a lot of money being allocated to secure the privacy of Australians. That is not specific to the health department; it is across the board. There are other measures.

Dr Richards—The protection of the privacy of the personal information held is fundamental to the public trust and therefore the participation in any health care programs. Clearly a significant amount of effort has gone into considering the regulations and the technical design components of any system which records sensitive personal health information. As Ms Murnane pointed out, the Health Insurance Commission, which does hold a significant amount of sensitive personal health information, has an e-business strategy. It has a highly secure internet gateway, which has been certified by the Defence Signals Directorate. HIC, I understand, regularly engages consultants which employ skilled hackers to penetration test their gateway, and to date no-one has been able to penetrate it. It is a highly secure gateway. I would expect any server that was storing personal health information in the HealthConnect environment would be subject to similar security requirements.

Senator STOTT DESPOJA—I might ask about that considerable effort. We have heard evidence today about a perceived lack of consultation in the roll out of this card. We are trialling it in one state. It really is under way now. It is not a question of it being considered. It sounds like this proposal is up and running, as a consequence of the minister's announcement on 28 July. What stakeholder groups or members of the public have been involved in the development of this proposal?

Dr Richards—I am not in a position to answer that question. I was not working on the HealthConnect project when the smartcard announcement was made by the minister.

Senator STOTT DESPOJA—I am happy for you to take that on notice. Thank you for outlining your understanding of the role of the Human Genetics Advisory Committee. I commend the government on its establishment. I am very excited about it. I would love to know more however. I am wondering if you can take on notice some specific queries. I have seen the budget papers so I know the general role and I also understand the allocation of $7.6 million over four years, but I would like to know who it is envisaged would be involved, who would be on the committee, what stakeholder groups would be involved if consultations took place to determine the membership of that committee and also whether it will be like other NHMRC committees in terms of determining a reference and getting references from the minister or whether it will have discretion to bring about its own references. Perhaps you could answer some of those questions.

Ms Murnane—We will take it all on notice.

Senator STOTT DESPOJA—I understand that this may not be determined at this stage. I ask that only because I am very interested in and quite excited about the whole thing. I might put further questions on notice.

Senator MASON—Do you believe that the federal Privacy Commissioner has sufficient powers to enforce the Privacy Act currently?

Ms Murnane—My beliefs are not really all that relevant but at the moment we have an inquiry into the Privacy Act. There has recently been tabled a review of the Privacy Act as it relates to the private sector, and that review was conducted by the Law Reform Commission and AHEC. There is always room for improvement. But I believe that the Privacy Act and the implementation of the privacy principles in the Australian government and comparable acts of

state governments have engendered a culture of privacy both within the public service and within the community generally, and the application of the privacy principles to the private sector has strengthened a policy culture there.

Senator MASON—Let me explain why your belief is important. If the executive is seeking to promote these e-health initiatives and, therefore, rely perhaps increasingly on the Privacy Commissioner, if they are not currently doing a good job or if they need further powers, your belief is important, isn't it? You are in a very senior position in the department. If you think that the Privacy Commissioner is not adequately protecting privacy, that would be relevant to a Senate committee, wouldn't it, about whether the Privacy Commissioner should be given more powers or the executive is promoting further initiatives? Of course it is relevant.

Ms Murnane—But I did not say that; you are imputing that. I have a bit of difficulty going on. I am not saying—I did not say and I would not say it—that I am of the belief that the Privacy Commissioner is not adequately protecting privacy. I am simply saying that it is a practice now, and a good practice, that all legislation and the relevance and effectiveness of legislation are reviewed at frequent intervals, particularly in areas like this, where community attitudes are changing and both new IT discoveries and, from our point of view, medical discovery and capability impinge on the external environment. There is a constant need to ensure relevance.

Senator MASON—So do you have any concerns about the Privacy Commissioner's protection of medical records?

Ms Murnane—No.

Senator MASON—The promotion of these new e-health initiatives and further responsibilities for the Privacy Commissioner, whether they are under a separate act or the same one, do not concern you?

Ms Murnane—That is a very broad statement. I would really want to know precisely what I was saying did not concern me. These are things that we give a lot of attention to. I am not willing or able to just give simple answers to—

Senator MASON—Let me make this clear: if you had said that currently you believed that the Privacy Commissioner was not doing an adequate job to protect medical records, the committee would be concerned to give further powers to the Privacy Commissioner if there were further e-health initiatives. All right? In other words, if they were not protecting medical records currently—if that is what you had said—the committee would be very concerned about giving the Privacy Commissioner more powers if you were seeking further initiatives. Okay? Do you follow that?

Ms Murnane—I did not say that.

Senator MASON—I know, but that is why I asked the question.

Ms Murnane—Okay; fine.

Senator MASON—Do you understand?

Ms Murnane—Yes.

CHAIR—Do you know how many complaints the Privacy Commissioner gets in the health area annually?

Ms Murnane—I do not know the answer to that.

CHAIR—I just wonder how you have come to the conclusion that there is no concern.

Ms Murnane—I think Mr McGrath knows.

CHAIR—You have made the assessment that you are not concerned about the Privacy Commissioner's workload in this area but you do not know what it is.

Ms Murnane—I do not know exactly what it is. Mike, can you—

CHAIR—Then how do you, Ms Murnane, come to that conclusion—not how Mr McGrath may come to a conclusion? Would you like to reassess your answer and look at some of the facts?

Ms Murnane—I will have a look at the exact number, but what I do know is that there is not a vast number of privacy complaints or breaches of privacy that come to our attention that cause a significant concern with the fabric of the system to protect privacy.

CHAIR—The Privacy Commissioner reports that she gets 330 complaints. You would not know how they have been handled, if they had been completed, or whatever, I would presume, if you do not know how many complaints there are.

Ms Murnane—I did not think we were here to be questioned on our views on the administration of the Privacy Act and the thoroughness and ability of the Privacy Commissioner and the Office of the Privacy Commissioner to carry that out. We see through a very small window into the work of the Privacy Commissioner.

Senator MASON—That is all we want to know about—your little window.

CHAIR—To a lot of people it is a very big window and a very critical area, and the way it has been administered by your department in terms of your information bases and also by the Privacy Commissioner in their capacity both legislative and resource wise to protect people's privacy is a critical part of this inquiry.

Ms Murnane—I am not sure what you are getting at. The Privacy Commissioner takes positions on what we do and put to her. We try to work with the utmost respect for the Privacy Commissioner's responsibilities and all that they are charged with. We would not say as a department that we have found deficiencies in the way the Privacy Commissioner carries out their task.

CHAIR—Sure, but that is a critical judgment and, when you say that, we on this side of the table draw conclusions from it. I asked you what you base that judgment on, and you were not

able to tell us the most basic information about the number of complaints and how they are handled. So for me that is probably a premature assessment that you made.

Senator STOTT DESPOJA—I want to make the point that this broad inquiry is looking at the adequacy or otherwise of the Privacy Act in relation to its current operations as well as contemplating the impact of new and future technologies. The department of health is in charge of arguably the biggest single technological device or change that will have an impact on the privacy rights of Australians, such as we have never seen before. The Australia card is nothing compared to what your department is in charge of. Looking at the potential consequences of this technology chills me to the bone. That is why today we need to work out whether current privacy laws are equipped to deal with this particular new technology and what steps the department and the government are taking to protect the privacy and security of Australians as a consequence of the development of this new technology. This is not airy-fairy stuff; this is happening in places around Australia, or at least being contemplated. We need to know who is involved in the process of determining these protections—so what public sector groups, what organisations, what industries have been consulted, if any. We have heard complaints about levels of consultation, particularly from the AMA.

Beyond that, my concern is whether or not this is going to be limited to the information obtained by departments or health professionals in relation to the HealthConnect card or whether there is a proposal to share information with other government agencies, a la the comments of Minister Hockey on 28 April this year that it potentially could be used in dealing with Centrelink, another government agency. To me, this opens up a Pandora's box of security implications and privacy implications, so forgive me if I am a bit startled by the notion that the department is not here to comment not necessarily on specific inquiries of the Privacy Commissioner but on the adequacy of the Privacy Commissioner's role and responsibilities now, including the act. I would like to put some questions on notice based on comments by the productivity commissioner that relate to whether or not the benefits of this technology outweigh some of the concerns that people have. Ms Murnane, you certainly have the right to respond to my comments.

Ms Murnane—I did say earlier that there is a continuous need to review legislation, especially legislation like this that is dealing with things that are important to people and that is at an interface with massive technological change and also change in medical biological discovery. The need to reconcile those is important. I am not in a position to say where exactly I think the Privacy Act should be changed. I think that is something that you are inquiring into. At the moment, we have been concerned that everything we have been doing is fully consistent with the Privacy Act, and we have been working very closely with the Privacy Commissioner and her office on that.

Senator STOTT DESPOJA—The department and obviously the minister have had the opportunity to examine the ALRC's comprehensive report into genetic privacy, *Essentially yours*. Can you advise us of what discussions, meetings or debates have taken place around that report? I am wondering if there is a time line for a response to that report. I am sure the minister is responsible for any specific dates or information, but I am just wondering what work the department has done on that comprehensive report.

Ms Murnane—The whole-of-government response is being developed. I cannot give you any more specific information than that, but we will look at that on notice.

Senator STOTT DESPOJA—I notice that in response to questions of mine in the parliament last week, Minister Ellison talked about specific aspects of that report being referred to the Standing Committee of Attorneys-General. I am just wondering if there is a comparable committee within the health department that may have been examining the report.

Ms Murnane—Not to my knowledge, but I will check on that.

CHAIR—Thank you very much, Ms Murnane and staff.

[11.28 am]

DRENNAN, Federal Agent Peter, National Manager, Economic and Special Operations, Australian Federal Police

VAN DAM, Mr Trevor, Chief Operating Officer, Australian Federal Police

WATSON, Mr James, Manager, Legal, Australian Federal Police

CHAIR—Welcome. Does submission 42 need to be amended or altered, and would you like to start off with an opening statement?

Mr Van Dam—With the chair's indulgence, we will make a brief opening statement. The AFP welcomes the opportunity to make a submission to the committee's inquiry into the effectiveness and appropriateness of the Privacy Act 1988 and to appear before the committee today. The AFP's submission to the inquiry was not a large one. We understand and appreciate the need for effective privacy legislation. We are happy that the legitimate interests of the community and effective law enforcement are provided for by the law enforcement exemptions in relation to the use and disclosure of and access to personal information. We have developed over a number of years a sound working relationship with the Privacy Commissioner and her staff based on mutual understanding and trust.

Our submission drew two issues to the inquiry's attention relevant to its forward-looking perspective. In our view, neither requires immediate action but we felt that it would be useful to flag them as the AFP will continue to monitor their development. The emergence of companies in the United States specialising in the collection and sale of publicly available information is a trend that we became aware of through our regular contacts with law enforcement agencies in the US. The new dimension is the increasing amount of information relating to an individual's activities that is available to be electronically captured and aggregated, which can go beyond the data that we would normally expect to see held by, for example, a credit rating agency.

The biographical profile able to be compiled from public source data about an individual can be based on tens, and even hundred, of thousands of pieces of information from public records and financial institutions. What is then available is a detailed history of that person from their birth, combined with a profile of their health, their lifestyle interests and their habits and behaviours which is continually updated. At present, we have little more information on this trend than that which was provided in our submission but we will continue to monitor developments in this area, particularly as it relates to the potential for identity theft, criminal targeting of individuals and/or institutions and the creation of false identities. We also have an interest in the context of potential impacts on our ability in the future to establish credible covert identities for members working undercover.

The other matter we raised in our submission was the occasional difficulty that we have experienced with some private sector organisations being unwilling to provide us with data in support of a legitimate criminal investigation and using the national privacy principles as a reason. We engage in dialogue with those organisations when this occurs, which often involves

educating them about the exemptions for law enforcement purposes. But in a small percentage of cases that is unsuccessful. Given the relatively mundane nature of the information, it is usually not something that we would want to pursue through more coercive avenues, such as a search warrant, which would also take up both our resources and the resources of the courts. We note the availability in certain investigative contexts—for example, proceeds of crime and ASIC investigations—of a tool in the form of a written notice to produce. We are continuing to assess that as an option we might look to pursue in more wide-ranging operational contexts.

CHAIR—Thanks very much. On that first point, what sort of information are we talking about—credit card records, flight records or what?

Mr Van Dam—In relation to the public source data?

CHAIR—Yes.

Mr Van Dam—That information that we see in the United States can be extraordinarily extensive. It can be birth records, it can be educational records, it can be places of residence, it can be credit card information, it can be purchase information where companies sell access to their client databases. That is why we make the point that what is qualitatively different here is not that any individual piece of information may not in itself offend a privacy principle but the capacity of new technology to allow organisations to compile tens, if not hundreds, of thousands of bits of information and then electronically sort and sift and use that to profile individuals to create a picture of the individual. That is where the emergent technology and the access to the information come into play.

CHAIR—Have you given any consideration as to how this sort of activity can be curtailed or contained?

Mr Van Dam—That is a very good question. What we are saying in raising it with you is that it is an issue that we have not seen emerge yet in the Australian context—not to the significant level that we have seen it in the United States. So we felt it was most appropriate to bring it to the committee's attention. We are not at this point suggesting a legislative or regulatory or other remedy, other than noting that the opportunities inherent here in a de facto way become opportunities for criminals.

Senator PAYNE—In your submission you say that the AFP intends to monitor this issue. How exactly do you intend to do that?

Mr Van Dam—In the Australian context we are part of the Opal Group, which has a national jurisdiction and covers jurisdictions and agencies across the Commonwealth. That group is, amongst other things, monitoring a range of domestic and international developments around identity crime. Through that group and the discussions of that group we are trying to identify emergent issues and bring them forward to appropriate policy agencies, against the backdrop of trying to support a whole-of-government approach to policy formulation in this area. The other area that we utilise to monitor issues is our high-tech crime centre, where we are actively engaged with law enforcement agencies in a number of countries to monitor the impacts of the development of new technology and the application of that new technology. For example, in our discussions with the FBI and others, we actively aim to monitor what developments are arising

in those countries and try to understand from their perspective what sorts of remedies and/or approaches might emerge.

Senator PAYNE—Is the FBI the appropriate link agency in the United States for the AFP?

Mr Van Dam—That is the agency with which we mostly deal directly.

Senator PAYNE—Have they put forward any suggestions for how to manage the issue in the United States?

Mr Van Dam—Not that I am aware of at this time.

Senator PAYNE—Thank you.

CHAIR—I will move to another issue, which you did not mention—that is, whether the AFP has been hindered by the Privacy Act. There have been some suggestions with respect to sex offenders overseas and the tsunami. Also, it was suggested that the Privacy Act provisions prevent Australian governments from providing to the New Zealand government the information of a person who has been released from jail but may be on parole or other conditions when they go back to New Zealand. I wonder if you have any comments with respect to those three issues.

Mr Van Dam—I will seek advice from some of my colleagues, if I may. But, first, can I preface this by saying that we in general terms support the position that the Privacy Commissioner has put to the committee, and we are very mindful of the Privacy Commissioner's comment that generally it appears that the construction of the law is considered reasonable. From an AFP perspective, we would support that position. In that context, in a general application of law enforcement or undertaking of law enforcement activities, we have no difficulties with the general construct of the act as it currently stands.

The matter you raise in relation to the tsunami is an interesting one in the context that the exemptions that currently exist allow for appropriate use in law enforcement circumstances. What we have seen with mass casualty situations—the Bali bombing being perhaps the first and most prominent one affecting Australia—was that the existing framework did not adequately protect or allow for the reasonable exchange of information where that was going to serve Australia's interests. In the past we have been able to achieve a legislative solution to that. So we would not necessarily say there is any fundamental flaw in the Privacy Act. What we need to be mindful of is whether or not the lessons we have learned from both the Bali bombing and the tsunami situation might lead to other remedies that establish more general principles and allow that type of information to be broadly captured within legitimate law enforcement uses.

CHAIR—Without interrupting you too much, could you take it on notice to inquire as to what the range of other remedies might very well be that we could consider as well?

Mr Van Dam—I would be very comfortable with doing that, and we will submit something to you on that. That is generally our response on the first matter. I will pass to Mr Watson on the other two matters that you raised.

Mr Watson—Thank you. The AFP, of course, is very careful in its disclosure of information to overseas law enforcement agencies, and it is important that we put that up front. However, within the legislative framework, the AFP is able to disclose information to overseas law enforcement agencies consistent with the provisions contained within the Australian Federal Police Act and in conjunction with the Privacy Act and the information on privacy principles. So we feel that, under the exiting arrangements, we are indeed able to disclose information to overseas agencies where they impact upon one of our functions.

CHAIR—Thank you.

Senator PAYNE—I am not sure that answers your question, though, Chair.

CHAIR—I thought it did, but you might have another aspect to it.

Senator STOTT DESPOJA—I did not think it answered it.

Senator PAYNE—The specific issue is: if a New Zealand citizen—

CHAIR—It might have been answered in respect of sex offenders.

Senator PAYNE—is released from detention on parole, leaves Australia and goes to New Zealand, the New Zealand authorities are concerned that the application of the Privacy Act means that individual's status cannot be revealed to New Zealand authorities and they cannot then accordingly manage the situation in both law enforcement and correctional terms. Whilst not agreeing or disagreeing with the view that they put forward, it is an issue that has been raised with us that we are interested in your response to.

Mr Watson—The issue of disclosure to overseas law enforcement agencies, in short compass, without dealing with a specific case—so forgive me if I am not across the specifics of the case which we are discussing—

Senator PAYNE—This is not a specific case; this is a general observation.

CHAIR—We are also talking about state criminal offences.

Senator PAYNE—There may be state criminal offences, indeed.

Mr Watson—As one of its functions, the AFP is charged with assisting in the investigation of the criminal law as it affects the Commonwealth. What that allows us to do is, in accordance with the confines of our existing Australian Federal Police Act, disclose that sort of information to overseas law enforcement agencies.

Mr Van Dam—I think the point about jurisdiction may also have a part to play here. It certainly would not be our intention to try and take matters away from the committee, but, if you would like us to, we would be happy to take that specific question on board and come back to you with perhaps—

Senator PAYNE—You are not taking it away from us. We would be very happy if you would provide us with further advice on that.

Mr Van Dam—From our perspective, we could give you what we believe the framework would be and confirm for you whether such a concern is real.

Senator PAYNE—That would be helpful.

CHAIR—Privately, we could pass on to you two or three instances where it is alleged to have happened.

Mr Van Dam—We would be very pleased to have that.

Senator STOTT DESPOJA—Mr Van Dam, in your opening comments you said that people were trying to use the Privacy Act as a shield, particularly private sector, I presume, businesses who did not want to give the information that you were requesting. You acknowledge that there are, I think, appropriate exemptions under the act, but you said there were still cases where people would not be forthcoming with the information. Obviously you have other recourse if you want to get that information, and you mentioned warrants and the like. Could I ascertain from you whether you arguing for a change to the act. Is there an educative role? Indeed, in reference to the Privacy Commissioner's report, are you happy with this recommendation:

The Office will work with the law enforcement community, private sector bodies and community representatives to develop more practical guidance to assist private sector organisations to better understand their obligations under the Privacy Act in the context of law enforcement activities.

Mr Van Dam—I will answer the last part first. The short answer is yes, we do support that recommendation. That is why we noted the education dimension in our submission. I will go back to your opening point. We are not suggesting, and our submission was not attempting to suggest, that people were trying to use the privacy principles in a multitude of cases to subvert. In fact, we make the point that, in many cases, that can be drawn back to their lack of understanding and their lack of confidence in the provisions and their ability to apply the provisions in a practical context.

In other circumstances, however, we do see cases where either organisations are concerned about a future commercial liability, for having passed information on, or they have been concerned about the impact on their commercial activities. Again, this is not wishing to be difficult, we have some specific examples but we are loath to raise them because, in many cases, we are still negotiating with organisations or entities to try to come to some agreement. That said, we are not suggesting that any legislative amendment or change is required to the Privacy Act. In the context of examining the possibility of notice to produce, we are aware of the fact that such a facility already exists within other legislation and that operates quite comfortably beside the privacy legislation. In some respects, it helps to clarify for a provider of the information that they have a cover in the context of a formal notice that gives them some comfort against future claim.

In our submission, we are flagging that we think it is appropriate to have a look at the application of that within some other legislative arrangements. Over the next period our view is

that we would examine that and have a look at whether or not, for argument's sake, changes to the police act or Crimes Act might be required. If that were to occur, our preliminary view is that that would not offend the Privacy Act in its current form at all. There are two reasons why we thought we would raise it. Firstly, we have actually raised it with the Privacy Commissioner in the context of her review, and we thought for completeness it was appropriate to put it on the table for the committee. Secondly, in the context of your term of reference (c), which is looking at the resourcing of the Privacy Commissioner, certainly from our perspective we strongly support the role of the Privacy Commissioner in educating the private sector and the community more generally about both their rights and their obligations in relation to the Privacy Act.

Senator STOTT DESPOJA—I have one final question. One of our submissions—the submission from the Australian Law Reform Commission—suggested that a new criminal offence be created in the case of nonconsensual collection or analysis of DNA samples. Do you have a view on that particular recommendation? I am happy for you to respond to that now or to take it on notice, whatever suits.

Mr Van Dam—I will confess that I have not had an opportunity to see the ALRC's submission, so it would be premature for me to give you an off-the-cuff response.

Senator STOTT DESPOJA—We will make sure that we supply that to you, and if you have a response that would be appreciated.

Mr Van Dam—Thank you.

ACTING CHAIR (Senator Payne)—The observations you made about the Privacy Commissioner's educative role really go, in some ways, to the second half of your submission in relation to the awareness of organisations in the private sector to the provision of information to you in a law enforcement capacity. What room is there to enhance the education of that aspect—the NPPs—of the Privacy Act? What role is there for the AFP, as opposed to the Privacy Commissioner, in doing that?

Mr Van Dam—In the context of earlier indicating our support for the submission of the Privacy Commissioner, I note that in the Privacy Commissioner's recommendations she has indicated that she will work with the representatives of law enforcement community private sector bodies to develop more practical guidance. We welcome that. From our perspective, we see this as a partnership. We do not take the perspective that it is solely a matter for the Privacy Commissioner to undertake that educative activity on her own. From our point of view, we remain pleased and enthusiastic about operating with the Privacy Commissioner in the development of guidelines and educative material. As our commission indicates, we are already undertaking a bit of that educative role on a case-by-case basis. As difficulties emerge, we then attempt to sit down with the entities who have concerns and work them through the provisions. It is one of those circumstances where it is not either/or. It will only be achieved through a collective effort.

ACTING CHAIR—I appreciate that, thank you. We have no further questions, so I thank you, Mr Van Dam, and your colleagues for assisting the committee this morning and for your submission. If you take that one question on notice, we will look forward to your answer.

Mr Van Dam—Thank you.

ACTING CHAIR—I thank all witnesses for attending and for their submissions.

Committee adjourned at 11.50 am