COMMONWEALTH OF AUSTRALIA

Official Committee Hansard

SENATE

LEGAL AND CONSTITUTIONAL REFERENCES COMMITTEE

Reference: Privacy Act 1988

FRIDAY, 22 APRIL 2005

MELBOURNE

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, 22 April 2005

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

Substitute members: Senator Mason for Senator Scullion

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, Ray, Sherry, Stephens, Stott Despoja, Tchen and Watson

Senators in attendance: Senators Bolkus, Buckland, Mason, Payne, 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 a.m.

CHADWICK, Mr Paul, Privacy Commissioner, Office of the Victorian Privacy Commissioner

CHAIR—Welcome. This is the first hearing of the Senate Legal and Constitutional Affairs References Committee inquiry into the Privacy Act 1988. The inquiry was referred to the committee by the Senate on 9 December 2004 and 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'.

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 of the Senate. We do prefer that all evidence be given in public, but under the Senate's resolutions witnesses do have the right to request to be heard in a private session. It is important that we get some notice in those circumstances.

I now welcome the Victorian Privacy Commissioner, Mr Paul Chadwick. You have lodged submission No. 33 with the committee. Do you wish to make any amendments or alterations to that submission?

Mr Chadwick—No.

CHAIR—Mr Chadwick, would you like to start off with a short opening statement, at the conclusion of which we will put you through a few questions.

Mr Chadwick—Briefly, yes. Thank you and good morning, Senators. Thanks for the opportunity to address you. I would like to make a few opening remarks following roughly the structure I set out in my submission when I posed some questions to you, deliberately taking what I call a satellite view of the issues. I am a specialist addressing generalists, so to me it seemed to be the most effective way that the relevant state or territory commissioners could address a committee of the federal parliament on an issue like this.

I have posed two questions to you. The first is: are the existing protections for privacy as you come to them now to look at an act that came out of a very different debate in the 1980s commensurate with the importance of privacy characterised as a human right as it has been since the Universal Declaration of Human Rights in 1948 and in all subsequent significant international instruments on human rights? The second is: is our protection in Australia sufficient for the balancing inevitably required when privacy is in play with other important public interests such as security, vibrant commerce and those sorts of considerations?

I thought that, in the words of an old television ad, I should say something about what the purpose of privacy is and what it is comprised of—when I say the old television ad, I am thinking of the old Palmolive ad where she says to him, 'Who'll tell you if I won't?' Who will tell the Senate about what privacy might be at its foundations if a privacy commissioner will not

at least try? So, without rehearsing some fairly extensive literature that grew mostly from the 1960s, with an awakening of what technology was likely to do to notions of privacy, I thought I would simply summarise, first of all, the purpose of privacy at its core.

Firstly, it is understood to be essential to selfhood—to the creation of the self. It is as fundamental as that, and it is why humans retreat to solitude at times or keep their reserve in the company of others. Secondly, it is understood to be fundamental to the creation and maintenance of intimacy between humans. Unless the privacy of your relationship with your nearest and dearest is observed by the partners, trust is lost. So privacy as essential to intimacy is the second purpose of privacy among humans. Thirdly, not to be downplayed but also not to be overplayed, is privacy as liberty. We can touch on that later if you wish.

My last point—which I think I should emphasise because this is happening a lot, and I notice some of the submissions to the committee, especially Ian Cunliffe's, have addressed this—is that privacy inheres in the natural person, not in governments or corporations or other types of legal persons. This is important because privacy nowadays tends to be misconstrued as secrecy and is used sometimes as a synonym for what we ought to treat as, for example, proper claims to commercial-in-confidence and proper claims to an exemption under an FOI act. Privacy inheres—in my view; it is not a universal view—in the living natural person.

I said I would say something about what privacy is comprised of. There are basically five dimensions. Firstly, there is privacy of the body: do not touch me unless I invite it. You are familiar with all of the laws around that, with body searches and, particularly and importantly, the remarkable developments in human genetics since the sequencing of the human genome in 2000. The second dimension of privacy is privacy of the home. I do not know about you, but when I get there I shut the door and drop the mask that I am forced to wear in public. That is where I can just be me. That is a place that is decorated in ways that reflect me—the photographs that I have around and whether I or my family are tidy or untidy. With the now cliched point about the home—that it is a person's castle—it is often forgotten that, in that standard case often quoted, the judge goes on to say it is a place 'for repose', not just for protection or dominion.

And the home, of course, is the place where the intimacy I described before is often played out. That is why it must be private and its privacy respected, and this is one of the reasons why people get so cross when telemarketers ring them at dinnertime: they feel they have left their life as a consumer at the front door and now they are doing something else. This is certainly the feeling that a privacy commissioner gets as he goes around the country, as he must, addressing the public. They are the single most asked questions: how did they get my number and why are they allowed to call me at dinnertime and address me by my first name.

The third dimension of privacy is privacy from surveillance: do not spy on me without just cause under law or without judicial oversight. Next, do not eavesdrop on me: do not listen around corners when I am having a tense discussion with my wife. There we can give three little episodes. A micro-episode you must have seen is the teenage daughter chasing the younger, naughty brother who has discovered her diary and is reading it to the family at the breakfast table. This is the micro example of privacy at work. A social example is the serious and interesting phenomenon that technologies of eavesdropping and of surveillance are now becoming cheaper and ubiquitous. The best example is, of course, the mobile phone with a camera in it, but there are others.

I have given a micro example, a social example, and I will now give a political example. The literature is now replete with the consequences on the social fabric and on a healthy political culture of excess surveillance of a community, and that literature has grown out of Europe since 1989. A splendid example is *Stasiland* by Anna Funder, an Australian. There is also a superb study by Timothy Garton Ash, a well-known English commentator on eastern Europe, in his book *The File: A Personal History*.

I have mentioned the body, the home, surveillance and eavesdropping. The last dimension of privacy is information privacy itself: the data trails that we all leave now as we simply live our lives. I leave one, and I may leave a more complex and digital one about my body in my medical records. That underscores the significance of smart Medicare cards or the HealthConnect program—something I am sure you are seeing in your other roles as legislators. With data trails about the home you have FlyBuys purchases, credit card data and property transaction data. Some people do not want it to be known how much they paid for their house or what they got for it, but there is a serious public interest there about a properly informed market.

I have touched on data trails about telemarketing. Regarding data trails about the home, there are more arcane applications—for example, police equipment that has led to a US Supreme Court decision and that can pick up body heat emitted from inside a home. So there are issues of surveillance in a virtual or non-visual sense, as equipment tracks a person or persons as they walk around their home. The case in question is called Kyllo.

With data trails to do with surveillance and eavesdropping, the obvious example is the data trails related to your mobile phone record—whom you called and when, and where you were according to the tower that was providing you with the service. Let us not underplay the public interest use of that data. It was vividly displayed in the New South Wales pack-rape cases, where data from mobile phone records was used by police to prosecute the young men who used to arrange the pack-rapes via their mobiles—or it was used to weaken their alibis. So let us not downplay the possibility of those data trails being useful in the proper enforcement of law, where warrants and other safeguards apply. I am commanded by the statute that I administer not to be an absolutist in relation to privacy but, instead, to try to strike workable balances. What tends to happen is that people expect the Privacy Commissioner on the public stage to speak only about privacy but not to recognise other public interests. I do not think that is healthy for the community we are trying to serve, because these workable balances and compromises must be struck.

The last significant aspect of information privacy—and it is not well understood—is what I call 'location privacy.' Lots of data about you locates where you were at a given time. This is particularly true now of transport technology, such as cars equipped with GPS. I do not know if Commonwealth cars are but it would be very interesting if anyone FOI-ed the data trails left by ministerial vehicles and other Commonwealth cars, to the extent that that would be kept by the GPS equipment in them. I am speculating there—I do not know if they are GPS equipped. But they leave data trails that will say where a car was. That is not, of course, necessarily where the relevant minister was—just where the car was.

Concerning tollways, we are increasingly developing tollways as a way of trying to provide better public infrastructure through public-private partnerships et cetera. Tollways record very significant personal data about people: their licence details; rego details; often their credit card

details, because of automated payment systems; and their patterns of travel—when they were using the tollway. That can and has been significant. In some American litigation it has been used to try to locate the allegedly unfaithful partner as not being where he or she should have been at the relevant time. So this data has power and needs to be considered in privacy contexts.

The last and I think very significant piece of technology that is relevant to location privacy and which is going to become more and more significant is something that the British are experimenting with and which has just been announced in Victoria on a trial basis: that is, automated numberplate recognition technology. In effect, it is technology that reads the number plates, in a very efficient way, of the cars travelling past the machine. Sometimes it is connected to the CCTV systems in that relevant—usually urban—locale. When matched with information about the persons associated with the registered vehicle, that can lead to very significant surveillance. I am not proposing to give a mini-briefing on that type of technology, but only to alert you, going backwards from that technology, to this notion of location privacy and the significance of it in the larger context of information privacy.

Why do I say the significance of privacy is growing? Why did I make that point in my satellite overview in my submission? It was for three main reasons: first, the significance of the Commonwealth Privacy Act is growing because information and communication technologies are growing, and so they should. They are useful, they are great for commerce and they can be terrific for public administration, but they bring with them some privacy issues which must be addressed, so the Privacy Act becomes more and more central. The second reason relates to international developments. It is sometimes forgotten that the Australian Privacy Act rests on the OECD principles of 1980, which were expressly designed to try to facilitate transborder data flows. Since 1980, of course, globalisation has continued apace, and data flow is critical to the proper functioning of all sorts of markets. APEC recognised this last year by endorsing a set of privacy principles based on that international model. That model is the basis for the Australian principles, for the Victorian principles and for the principles in the much more developed data-protection law of Europe.

The third factor that explains why the Privacy Act is growing in significance is 11 September 2001 and what has flowed from that in terms of public policy. We are now recalibrating the balance between liberty and security. Privacy is legitimately a subset of liberty, and those of you who have had to address things like the ASIO legislation et cetera will be aware of those arguments. They were beautifully adumbrated by the House of Lords in its recent debate over the prevention of terrorism bill in Britain. It was a very unusual, non-partisan debate in the House of Lords, and I commend the transcript to the committee and its researchers.

The submission notes the hybrid rationale of our privacy laws. People tend to think, 'This is Australia's way of putting into domestic law this grand and highfalutin human right of privacy.' It is more than that, and it is pragmatic. It has an economic driver, and that is certainly an overt part of the Victorian information and privacy act. The then Victorian Treasurer devised it. It was not some you-beaut human rights committee of the parliament or something; it was the Treasurer who recognised in the nineties—and the subsequent government in 1999 took this on; it is a bipartisan effort—that, unless we convince the public that their privacy is respected, they will not engage with the IT that we know can improve public administration, which we call e-government, and commerce, which we call ecommerce. People will not engage—this is a

universal, resounding result of the surveys and other things. They will not engage unless persuaded by their leaders and their legislature that their privacy is protected.

That leads me naturally to the recommendations. I will not touch on any of them now in this opening statement, but I underline that one aspect of maintaining and developing that trust is having a strong, properly resourced, independent Privacy Commissioner's office. That is one of your terms of reference. It is of course invidious for me to in any way speak for my federal colleague. All I wish to say is that my own experience is that it is critical that whoever is Privacy Commissioner has a strong law, making him or her genuinely independent; it is critical that he or she has access to appropriate resources, or else they suffer a kind of bureaucratic anaemia; and no-one can help you with the last thing that is critical to an effective statutory officer, which is for the character to be genuinely independent. You as legislators cannot help anyone with that, but you can certainly help on the first two. Thank you for your attention.

CHAIR—Thank you, Mr Chadwick. We have more than enough questions for this morning. I start off by noting that when I introduced legislation leading to the Privacy Act in 1987 my greatest supporter in cabinet was the then Treasurer Paul Keating. We had to bat off all sorts of portfolios of commercial interest, including Treasury.

Mr Chadwick—Can I ask whether the Treasurer's support was founded on this idea that you have to build confidence in order to get the technology humming for commercial and other reasons?

CHAIR—I think, strangely enough, it was a combination of that together with an interest in protecting people's privacy. So there was a pure motivation. Whereas Treasury, Finance, Industry and Commerce and whatever wanted to introduce positive reporting at that stage, he and a small handful of others were very strong in balancing the introduction of any such reporting system. So maybe he shared something with the Victorian Treasurer. I suppose the point is that support for this issue of privacy comes from strange quarters sometimes, and that, thankfully, was one of them.

Drawing on that experience, since 1988 the legislation has stood in place, but we are finding on a day-to-day practical level that maybe it is not as effective as it was. The capacity for people to waive rights is one thing that we find daily. You mentioned data marketing. I have had instances recently where Origin Energy people have rung me as a supporter of a particular football team to tell me that I can get a concession on my energy costs. Not only was I offended by their background knowledge, but they also got it wrong. All these things—waiver, technology and so on—lead to a concern in my mind that some of the specifics of the act need strengthening. Even though we are generalist we need to get to specifics.

I note in your conclusion you recommend harmonisation of federal and state legislation—IPPs in the public sector and NPPs in the private sector. You also recommend greater transparency and you refer to the Californian 'shine the light' law. Could you mention the importance of those two recommendations and whether they are the hub of what we should be looking at in terms of our recommendations.

Mr Chadwick—I will leave the latter part of the question aside for the moment. If I forget about it, please remind me. On the former part, I think there is no question that it needs

renovation. You crafted it in the eighties—and it was interestingly bipartisan then too—in a different context. The speed with which information and communications technologies are coming to the market now is extraordinary, let alone when they become available to the arms of government. It needs renovation. One useful thing would be to take those moves of roughly the years 1999 to 2000-01. The senators will correct me, but I think Daryl Williams was Attorney at the time. You covered the private sector with basically the international privacy protection principles that you find all over the world and that come from the OECD principles of 1980. More or less, you covered the private sector with that.

It would be good to harmonise those principles as a result of this review. I would add my voice to the many that are urging that. It is practical because it means that these generic, open-textured principles can at least be thought through and a coherent body of law can be developed for the public and private sectors. One reason why that is so significant is that, of course, since 1980, a dramatic change has happened in what used to be the sharp barrier between the public and private sectors. Many public functions are now provided by the private sector through outsourcing and, in the most dramatic examples, privatisation. That means that the public is sometimes reacting to a request for personal information made by government under law for a public task, but the practicalities of protecting that data and keeping it accurate et cetera are happening in the back office of a contracted service provider, sometimes offshore. So it just makes sense to have one set of principles with enough flexibility for the relevant decision-makers to apply them intelligently in the many different settings in which you find them.

I would make one point about this. The protean nature of information is very poorly understood. If you would allow me, I will make just one simple point to illustrate this. These principles are meant to be generic because it is impossible—as you, Senator Bolkus, and the other architects of the act would have known—to craft detailed law in this area because information itself is so protean. The best illustration is this: my name means one thing in the phone book, another thing on the Australia Day honours list and another thing again on a sex offenders register. But it is the same information. In that trite and hopefully dramatic way I have illustrated the protean nature of information and why you need generic, open-textured principles such as the OECD gave us all. Those principles were recently reaffirmed in a meeting of ministers in Toronto, I think it was, in 1998. They said that the OECD principles still work although they have to tinker with them. I think we need to do that here in Australia.

I would affirm that we need to bring them together. The IPPs that govern your Commonwealth public sector hail from the eighties and I think they can be usefully brought together into one set of principles applicable across all areas, with a couple of tweaks. One of those might be where somebody wants to offer an opt-in, opt-out option to other users of your personal data, say, for direct marketing. The compromise, as you know, of the Commonwealth parliament was that, with the private sector, the compromise is opt-out. You can try; if someone says, 'Can you take me off the list,' then you should. That was your compromise. But I am not sure that that is the appropriate compromise where the state has compelled a person to provide the data—for example, for the electoral roll or to the ABS in a census. If the state compels the provision of personal data for a set purpose, I am not sure that it is appropriate to then allow the state, as it were, to leverage from that wonderful data set into commercial uses without saying, 'Here we need to tweak it so that it is an opt-in,' so that you allow the person to say, 'Yes, you can have my data for the electoral roll or whatever it is and I will tick the box to show that I do not mind being marketed to.' That is an opt-in.

CHAIR—I remind you of the second part of the question—the 'shine the light' legislation.

Mr Chadwick—Yes, thank you. Governor Schwarzenegger recently signed the law in California for what is called the 'shine the light' bill. Essentially, as I understand it—I have had a cursory briefing from my own staff, but I have not read the actual text—it requires commercial entities to tell people what they are going to do with their personal information and who they give it to habitually.

It is an attempt to allow people to answer the question, 'How did you get my number?' They say, when the telemarketers ring at dinnertime, 'How do you know this number?' Sometimes they say: 'I have a silent number. Where did you get this?' The aim is to have more transparency. I think transparency is a greatly undervalued tool in this area of privacy—and that is partly because it is counterintuitive. To think of transparency as useful in the realm of privacy seems counterintuitive but, in fact, it is built into the law I administer. It is in the 'objects' section—to try to make the public sector administer personal information responsibly and transparently. That is because, where there are other uses of a person's personal information that are in the public interest, one way you maintain their trust is to be open about what you are doing with it. A lot of people will say: 'That is fair enough. It sounds all right to me—I just wish you had let me know.' So transparency is built into most of these laws.

The other bill in California is a companion piece of legislation. Where an entity becomes aware of a breach of its personal information holdings, particularly where it puts its customers at risk of identity fraud, it is compelled under law to alert people as soon as it can. It is a very interesting, pragmatic tool. Accidents happen, rogue employees do the wrong thing or someone walks out of the office with 10,000 names and addresses—or whatever it is—on a CD, because the data is very fluid. And when the entity learns of this it is compelled under that Californian law to try to alert its customers, 'Watch out, your identity may be misused in a fraudulent sense because this has happened to us.' I see some value in that companion piece of legislation as well.

Senator STOTT DESPOJA—Just going back to Senator Bolkus's Privacy Act—without wanting to in any way detract from the formidable role that my colleagues played at that time in devising the act and without forgetting the fact that they had Michael Macklin snapping at their heels—that whole debate in 1987-88 played out against the backdrop of the Australia Card debate. I am just wondering, in today's context, how you would assess the views of the public towards that broad issue of privacy and privacy rights, if you like, or how you would assess people's concern about the balance between security, for example, and privacy? I am wondering if there is a comparable view of 'Oh, my goodness, my personal details are well known,' or 'There are these rapid advances in technology that may affect my privacy.' Is there that level of concern in the community now, or is it a bit more amorphous—you cannot really assess it?

Mr Chadwick—The specialists are having troubles, so it would not surprise me if the ordinary member of the community is really astonished but is without a coherent view on a lot of these developments. Sometimes I use popular culture as a barometer: which television shows rate? It is very interesting to see the popularity of programs that use information technologies to solve crime. I am thinking of the program *CSI*.

Senator MASON—I thought you were going to say *Big Brother*!

Mr Chadwick—That is slightly different. Let me put it in shorthand. It is very interesting that people appear to love *Big Brother* now, contrary to the climax of Orwell's novel, where it is deeply ironic and scary. And yet *Big Brother* the program and the idea of ubiquitous surveillance and watching someone en famille, or 'at home', is the reason for the show. Can I say something clearly, because I am on the public record: that show is harmless, as the participants have clearly consented. It is a piece of fluff; it is a piece of entertainment. What is interesting about it is that the name does not chill the generation that came to the phrase 'big brother' through that TV show in the way it chills most of us—I cannot speak for everyone—who came to an understanding of the phrase 'big brother' through Orwell's novel. This is interesting in itself because of the way Orwell deals in that novel with the use of language in politics, and he does so in his other essays as well. The language has changed; *Big Brother* is loved. It is a piece of amusement for some people.

The other thing I would like to point out about the program is that my kids watched it, as many people's did. I noticed that even though its founding notion was ubiquitous surveillance and the young adults who made up the housemates were generally all consenting, when one woman got really upset once and the other women were trying to comfort her, according to the voiceover—and I say that advisedly—the women took her to a spot in the house where they believed the cameras could not see her. That is a really interesting and vivid example of the deep human need for privacy. It reminded me of that wonderful opening to *Nineteen Eighty-Four* where Winston wants to begin his diary but he has to work out a spot in his flat where he cannot be observed by the telescreen.

On the general view, the public talks to me about it, but I am the Privacy Commissioner, so you would expect that. They probably talk to you in electorate clinics and in all sorts of other contexts from your professional lives. I notice that they respond very strongly to questions of access to their personal information, particularly their financial and medical information. I do not need to say to this group that that would translate into their votes if they got cross enough, but you all know that. The thing about the public's reaction in Roy Morgan polls conducted by the Federal Privacy Commissioner in 2001 and 2004 was that they were open to the benefits of the technology, according to these results, but very strong about insisting their privacy be protected. It is an incoherent expectation, as you would expect from generalists, but it is a real expectation. What hurts both public and private bodies are these stories that appear where they say, 'We've lost this data' and it is on page 1 and everyone is in damage control.

It is much more sensible for public sector and private sector entities to follow these data protection principles, because they are not just about use and disclosure of data, they are about collecting only what you need. You do not have a problem if you have not collected it. They are about keeping it secure and keeping the data quality high. That is important because, as you know, both private and public sector entities, if they are dealing with dirty and inaccurate data, will often infer the wrong thing and make the wrong decisions, with real costs in remedying the situation and sometimes real harm. So the principles are poorly understood, partly because of the lobbying around the private sector amendments of 2000 and partly out of the misuse of privacy as secrecy. There is a lot of what we call in the trade BOTPA—a word devised by the former New Zealand Privacy Commissioner, Mr Bruce Slane, who was for 10 years their commissioner. He is a fine lawyer and formerly the head of their broadcasting authority. He developed the term BOTPA, and I asked him, when I was appointed, 'What's that mean, Bruce?' He said: 'Because of the Privacy Act. You will find many incidents of people saying, "We can't give you that, we

can't give you this, Because of the Privacy Act," and it won't be because of the Privacy Act. It will be something else.'

Senator STOTT DESPOJA—What message are we sending to the public when we have a Privacy Act that obviously covers the public and now private sector but we have exemptions—for example, for political parties? Do you have a view of that particular exemption and is there any recommendation that you would like to make to the committee about it?

Mr Chadwick—I do have a view. It is the same view I put to the Victorian parliament. All of you know better than me—and of course I do not make this comment either gratuitously or in a partisan fashion—that there is a deep literature about public trust in public institutions. One aspect of trust is the willingness to submit to the same levels of accountability as everybody else, particularly the ones you impose on everyone else. I think that the political parties' exemption needs attention because of that. There are mechanistic reasons why it needs attention—for example, the sophistication of the databases that your different party organisations maintain. They are often full of fine-grain data about the community, which you legitimately need, I think, to run a democratic community properly, to fight tightly fought election campaigns in marginal electorates and all the rest. You need that. But you need to be much more open about what you do. I think you need to apply to yourselves two basic principles: you have to be more transparent about it, and you have to let people see what you hold about them and correct it if it is wrong. I hope I am understood when I say that in my public role and without any trace of partisanship. I apply it to all political parties. It would be good for the credibility of the parliament and the political process if all the parties would address this question of your preferential treatment under the Privacy Act.

Senator STOTT DESPOJA—Perhaps in your answers to other members you could speak on anything you think of in relation to the protection of genetic information. You have given us a comprehensive submission, but you know I would have liked to ask you about that, with my particular interest. I am not sure if at some point you could give us an idea about how well-equipped the law is to deal with not just emerging technologies, to which you have referred in your submission, but microchips. That is something I would have been interested to know about. Perhaps you could take that on notice.

Mr Chadwick—Certainly.

Senator MASON—Let me bounce off Senator Stott Despoja's incisive questions. Do you think that the public values privacy less today, or is it simply contextual? Let me explain. Back in 1986-87, in the Australia Card debate, privacy was one of the key terms used by opponents of the Australia Card to challenge and finally overcome that legislation. I think it is fair to say that at the time that the proposal was first mooted it was generally supported but over time public opinion moved against it. Privacy was one of the words used to defeat it. It was used again in the human rights sexual conduct legislation, to overturn homosexual law reform in Tasmania. Again, privacy was used as the legal but also the philosophical tool. Recently, with the current debates post-September 11 and post-Bali—you mention this in your satellite view—I participated, and Senator Bolkus, Senator Payne and senators here participated, in a debate where we gave the Australian Federal Police and ASIO greater powers than they have ever had before. That was far more substantial, in many ways, than the Australia Card proposals were. Yet there was hardly a

whimper. Perhaps I should not say that, but in the political context in parliament privacy barely got a run. Are you concerned about that?

Mr Chadwick—I have to be, but I have to be wary. When someone's daily bread is the question of privacy, you have got to be careful that you do not see the world through privacy-coloured glass. You must have this—when there is a hot political issue you see it everywhere. I have to guard against seeing the world in terms of privacy threats or privacy protections. It would drive you mad, for a start. So I am always checking myself and saying: 'What is the public view here? Are we over the top with this?' On the other hand, I have got to animate public functions, give advice on privacy points, make the public aware and all the rest. I think we are going through a recalibration of liberty and security. I put it at that elevated level. It has happened since 11 September 2001 in many ways. It has in some ways been my privilege to be an observer of that process, not just in Australia but among my international colleagues. It is happening everywhere. We all talk about it. There are some basic guides that I think are worth following. One is that you should follow proper process, and not too hastily. One of the most disturbing things is the speed with which some of these laws have been passed and the absence of what I would call due legislative scrutiny.

Senator MASON—Both here and in the United States and Great Britain?

Mr Chadwick—You can see the Congress rethinking aspects of the PATRIOT Act, for example. In Britain, one of the strongest parts of the debate in the House of Lords over the recent Prevention of Terrorism Bill, which is not a minor matter—I think you know it; it was essentially the permanent suspension of habeas corpus, a very significant debate—was, interestingly, marked by a lack of partisanship. I am talking about the Lords. The Commons was, as normal, whipped by party discipline.

Senator MASON—Those in the House are always better agents of scrutiny, isn't that right?

Mr Chadwick—In the Lords, you would get a former Home Secretary get to his feet, or a former Secretary of State for Northern Ireland, and begin by saying, 'My Lords, I have interned people,' or, 'My Lords, I have spent half of my career receiving briefings from the security services.' It was a way of laying, in a rather understated fashion, their credentials out at the opening of the debate. What you found was that many of the lords would come back to the idea that you must have due process and not be hasty, you must try to put in sunset clauses where you feel that the atmosphere of the time is perhaps distorting judgment or you are really going a long way and you might want to revisit it as a parliament soon and you must ensure that you have independent oversight—a genuine role within its constitutional limitations for the judiciary, for example, and, in the case of Australia, a proper role for the oversight bodies. One of those bodies is the privacy commissioners, but they are fairly small in the scheme of things. There are also oversight bodies—for example, the parliamentary committees that oversight security or the relevant oversight ombudsman, I think it is—for the security services at the federal level. So be aware of the safeguards and keep in mind questions of necessity and proportionality.

Keep sunset in mind and, going back to Senator Stott Despoja's question, keep it in mind especially in the area of genomic data. Be humble about your ignorance. A lot is being said about what the sequencing of the genome will allow us to do or not do. We are in a time which vividly recalls to me the early years of the 20th century in the US when eugenics got such a head of

steam up that it began to infect public policy making in ways that were grievous and that are now known to be grievous. So, on the genetic point, I see that as a premier privacy issue for this committee to address. It is highly specialised.

One way where you can be practical is to be very wary of the so-called scientific certainty—the illusory certainty of science—when it is applied in a forensic context. That is one area where I think we need really clear structures, and we have not got them yet. For example, it is possible for the state to collect bits of your DNA outside of the forensic procedure structures of the laws of this country. That, I think, is a woeful lack that needs immediate attention. The data contained in my DNA, not just about me but all my blood relatives, is possibly highly revealing, which we see as we learn more about the genome. I have said this in other contexts but I hope it is vivid enough for you to carry it away. John Donne was right. No person is an island. Genetically speaking, each of us is an archipelago. The power of that requires reflection because privacy is quintessentially associated with the enlightenment and the idea of the rights of the individual. But here we have collective privacy.

Senator MASON—We could go on all day, but I expect this theme will run through our discussions over the next few weeks. Perhaps you cannot comment on this because it might start a long philosophical discussion, but a lot of literature posits the enlightenment distinction between the individual on the one hand and the state on the other. I am not certain that that is an appropriate distinction. People are too quick to jump to the situation of privacy of the individual versus the security or the interests of the state. I do not think the distinction is that clear. I think there is a merging, and there has been merging in more recent times. How is that for a debate?

Mr Chadwick—I think that it is impossible for us to pursue that, but I must ask you: how far has the individual now merged into the state, in your view?

Senator MASON—I will give you a quick example—the clearest one, perhaps. You talk about the liberty of the individual and the privacy of the individual. There is no greater infringement on the privacy and liberty of an individual than molestation by someone else. If that molestation requires, in some cases, extra security, security and liberty are not antithetical. It is not one versus the other; it is a merging of interests. The primary role of the state is to protect individuals.

Mr Chadwick—I would not contest for a moment that many compromises are necessary—some of them very significant compromises of privacy—in order to protect the vulnerable. You are alluding to that.

Senator MASON—This debate sets up one versus the other, and this is what I do not accept. I do not accept it is one versus the other.

Mr Chadwick—I understood your initial remark to be that the state is somehow subsuming the individual or that the individual is not so separate from the state.

Senator MASON—No, I did not mean to say that.

Mr Chadwick—That would confound a lot of literature and recent experience in other parts of the world.

Senator MASON—I was saying that the intellectual debate has been set up as being that the individual's interests are always antithetical to that of the state's in the context of privacy. I think that assumption is wrong.

Mr Chadwick—Put in that simple way as the opening in a conversation that would explicate the point, I would be happy to engage in that conversation. But I suspect that we cannot do it now.

Senator BUCKLAND—We could debate every area of this with you for hours, Mr Chadwick. You made very fleeting reference to privacy in the workplace. How far can you take that? More and more we see people having to divulge more about themselves to gain employment and then that information being devolved through the lines to their point of employment. Things like sexual preference, marital status and religion have no bearing on your ability to do a job, and of course there are others but time does not permit us to go into them. How far can you take privacy in the area of employment?

Mr Chadwick—At its core privacy is about the dignity of the individual, and we must attend to his or her dignity as a working person in their working environment. But there are very pragmatic reasons why we might constrain privacy in certain working environments—for example, where there is a high need for data security or a high need for physical security, or where they are working with objects or products that might be susceptible to misuse. I am thinking of having higher requirements to know about people when they work for, say, the security services or in certain aspects of the police force, or when someone is entrusted with control of large amounts of money or, in the medical context, with large amounts of drugs.

There are many ways in which workplace privacy needs to be calibrated to suit the circumstances. But the general answer is that a person is a person whether he or she is at work or elsewhere, and their privacy matters to their dignity. In the industrial revolution one of the aspects that led to people being concerned about the treatment of working people was a negation of their privacy—for example, toilets without doors, so that they could be inspected to see whether that really was a call of nature, and those sorts of things.

We have high-tech ways to surveil people—for example, workers carrying those key tags that get you through a door, which we are all familiar with. If the system needs to track them as they move around the building, it is very important to people's dignity that the system does not track them when they are in the loo, even in that virtual way. So I think employers, who in my view are ordinarily people of goodwill—

Senator BUCKLAND—That is debatable.

Mr Chadwick—In my experience a lot of the people actually managing entities do not want to negate the dignity of their workers. That is my experience anyway, and I am sure that other people will have different experiences. But when a company is receiving marketing from a technology company saying, 'You really need our systems, because they're going to ensure that people come on time and you will know when they are coming in and going out,' and it involves biometrics or something of that nature, where the person feels physically vulnerable to something scanning their eye—really human reactions to this stuff—that is where managers

need to say, 'Look, do we really need it like this? Can we secure the place appropriately without actually putting people through all this and, anyway, is it worth the cost?'

There is a lot of really potent marketing going on for some of these so-called technological solutions to issues like workplace security, and when you scratch them a lot of them either do not deliver what they offer or are disproportionately intrusive. You can achieve the thing that the employer wants without such an intrusion. The other thing to think about is that we are going through a period in which the work force is using technology sometimes to work from home, so you are conflating the workplace with the home. As I said in my introduction, the home is a very special place, and that needs to be considered by policymakers.

Certainly I would urge the committee to rethink the employee records exemption and to think in a holistic way about workplace privacy. It is bobbing up all over the show in the Australian states. New South Wales has had a go and Victoria has a Law Reform Commission inquiry going. People are scratching their heads about surveillance cameras—for example, when they are used by voyeurs. Employers set up the cameras but unfortunately they sometimes use them for voyeuristic purposes in relation to women employees or something like that.

Senator BUCKLAND—Is it really about defining the line where privacy and dignity are crossed, or is it broader than that?

Mr Chadwick—Respect for privacy is facilitative of the individual human's dignity, and we stand for that in this community. We stand for the idea of respecting that.

CHAIR—That is a good point on which to end. This has been a good way to start this proceeding. We thank you for your evidence, verbal and written.

[9.51 a.m.]

KUMMROW, Ms Joanne Maree, Solicitor, Administrative Law and Human Rights Section, Law Institute of Victoria

O'SHEA, Mr William Patrick, Council Member, Past President, Law Institute of Victoria

SAMARARATNA, Mr Nihal, Member, Law Institute of Victoria

CHAIR—Welcome. Do you have any comments to make on the capacity in which you appear?

Mr O'Shea—I am a solicitor and I was President of the Law Institute of Victoria in 2003. I am also a corporate counsel at Bayside Health, which is the health network in Victoria which operates the Alfred, Caulfield and Sandringham hospitals.

Mr Samararatna—I am an articled clerk at Best Hooper Solicitors in Melbourne and manager of Goonawarra Medical Centre in Sunbury, Victoria.

CHAIR—You have lodged submission No. 37 with the committee. Would you like to make any amendments or alterations to it?

Mr O'Shea—We would like to give a short summary of it but we have no amendments. We are grateful for the opportunity to appear here this morning and that we have been given the opportunity to make this submission. At the outset it is important to say that in Australia we have no right to privacy. We have no bill of rights and therefore we depend on the legislature and you, as our law-makers, to ensure that whatever laws we have on privacy are fair and reasonable and protect people's human dignity.

As we said in our submission, the Law Institute's view is that an individual's privacy is fundamental to their human dignity, as Mr Chadwick has already outlined this morning, and is central to other human rights, such as the rights of freedom of association, movement, speech and, indeed, freedom from unwanted surveillance and intrusion. In preparation for appearing here this morning, I have just spent two weeks in Berlin on leave. I visited the headquarters of the Stasi in East Berlin, which are now open to visitors—not only the headquarters of the Stasi but the prison where they remanded people and interrogated them in order to catch up on the surveillance they had obtained on them.

If you have read *Stasiland* you will know some of the issues that that surveillance involved. The files that they collected on people in East Germany are now being put together, having been shredded, and will take 240 years to be reassembled so that people know what files were collected on them. The operation of the Stasi is an excellent example of the right-hand end of the spectrum on the individual's privacy and the right to privacy and human dignity that was so brutally attacked in East Germany from 1945 to 1989. It is a very illustrative example of the position you as legislators are in when you start to look at the balance between the rights of the

individual and the need to limit those rights for various purposes. It is particularly important that we act conservatively whenever we propose to limit rights.

Of course, lawyers are renowned for taking a human rights perspective on things. I urge you not to dismiss that because we are lawyers. In a sense, lawyers are needed in the community for the very purpose of putting unpleasant submissions, and often we defend the indefensible. That is very important, because if you do not have that you do end up with the Stasi running your country. So I urge you not to dismiss us because we say to you that we think the default position is that you do not impose restrictions on people's privacy. The default position should be not to do it. It should only be if it is necessary.

In terms of specific issues in our submission, I draw your attention in particular to the fact that we believe that the act is falling behind new technologies and needs to catch up, particularly with smart cards, genetic information and biometric encryption. It is clear, and I do not think I need to elaborate, that the act needs to catch up on that. In terms of business, our submission deals with the need for Australia to have a privacy system that complies with the EU directive. It is particularly important for Australian businesses that are collecting information and want to deal transnationally. If we do not comply with the EU directive, Australian businesses are going to be impacted in terms of the extent to which they can work offshore and deal with other jurisdictions. At the moment, our privacy regime does not meet the EU directive. In terms of biometric encryption, we do not believe the technology is secure. If the technology was secure, we would be more comfortable about biometric encryption being used. However, we believe it is still subject to hackers and interception, and we urge caution in terms of allowing biometric encryption in Australia until that technology improves further.

In terms of genetic and genome information, we are strongly of the view that insurance companies and employers should not be able to deny insurance or employment by having access to genetic information. We believe genetic information is personal to the person to whom it relates. If that person consents to that information being made available, that is fine, but we do not believe that an employer or insurer should have the right to compel a person to disclose that information. That, of course, is subject to the ability of the business to operate. Clearly there will be some examples at the margins where a business cannot operate if a person has a particular characteristic. However, as a general rule, the default position should be that that information is not made available and there is no obligation to make it available. That is a summary of our position.

Senator MASON—It is common for legislatures today to consider environmental impact statements when they are considering legislation. You argue in your submission that there should be privacy impact statements. How would they work, and do you think they would have been of great benefit in the recent debate in the Australian parliament about the security legislation passed after September 11 and post Bali? I mentioned to a previous witness that, while privacy was argued, it was not argued very much in that debate.

Mr O'Shea—I was president of the Law Institute while that legislation was put through. The Law Institute ran a number of public seminars on the ASIO legislation. We wrote to senators, including Senator Faulkner, who was leading the opposition's case on the ASIO legislation, and received no reply. I do not know what the mail system is like in Parliament House, but for you to

say that there was no concern about that legislation is incorrect. It might be your perception, but it was certainly not—

Senator MASON—I mean it barely entered into parliamentary debate, which is a different issue.

Mr O'Shea—I can understand that, because none of the issues that we raised were ever acknowledged. I presume the letter never got through. We had public seminars, certainly in Melbourne. I cannot speak for the Law Society of New South Wales. The seminars were extremely well attended. We were subsequently interviewed on national television. We were, and remain, very concerned about the ASIO legislation.

Again, our view is that it was modified largely through some of the pressure that was brought to bear by us. You will remember, I am sure, that the legislation was amended to reduce the time of cross-examination without legal representation. So I think there was some recognition of the fact that there was public concern about it. In terms of the assessments and the privacy impact assessments, there are various ways that could be done. For example, if Medibank Private or Medicare were to change the way they collect information on behalf of members we would expect that an impact statement as to what that change would be would be provided to all members. If that were to go through parliament we would expect that impact statement to be part of the legislation, certainly either incorporated in the second reading speech or made available to the public.

Senator MASON—Or in a cabinet submission or whatever.

Mr O'Shea—Indeed. If there were other examples where legislation was not required, we would expect the peak body for the organisation that had that information to provide a privacy impact assessment for those people in the public who were dealing with it. If, for example, it involved the Insurance Council of Australia we would expect to be required to produce for the public a privacy impact assessment of whatever they were planning to do.

Senator MASON—Do you think that if there had been a privacy impact assessment on, for example, the ASIO act, that that would have tempered the enthusiasm for the cabinet's initial endorsement of the first bill?

Mr O'Shea—It might well have done. You cannot underestimate public apathy. You can go so far and you can give them lots of information but in the end there is apathy about it. There is an inherent conservatism in the Australian electorate. The Eureka spirit is much weaker than it was 150 years ago in Australia. I would say that it is still there, and people believe that when things are tough it will re-emerge. But I do not think we should underestimate the value of putting those things out. I think the fact that there is apathy and that Australians might appear to be disinterested in it are not arguments saying we should not do it.

Senator MASON—I have no further questions, except to say by way of comment that privacy is a politically contestable right. In effect, that explains the tumult of the Australia card and also the apathy with respect to security legislation. I just say that by way of reflection—I might be wrong.

Mr O'Shea—A point I did not make before was about smart cards. We are concerned also about the linking of information through smart cards. One of the problems with smart cards is that often people do not know what is actually stored on a smart card and therefore how to access what is there, nor do they know who is going to get the information on the smart card. In a sense, that was part of the concern about the Australia card as well. We would be very concerned about any inability under the act to deal with this issue to prevent that happening. There need to be strong restrictions on the use of the smart card. Just yesterday we saw Minister Hockey making an announcement about the possible use of smart cards to link this information. We believe that is inappropriate and we would oppose it. We are not saying that we therefore support welfare fraud. We are saying that there is a more fundamental issue at stake here and that is that smart cards should be used sparingly and only to the extent that it is absolutely necessary.

The default position should be that we protect people's privacy and that you as legislators do the same. That should be our position. Otherwise, I do recommend you go to the Stasi museum in Normannenstrasse in Berlin and have a look at what they got up to. If we have a drift in this community based on 9/11 or the US alliance or whatever else we are concerned about the drift will inexorably be to take away people's dignity and progressively take away more rights by privacy infringement creep. We have to be aware of that.

CHAIR—Before I move to the next senator, Senator Mason, I ask you to reflect on the inquiry into ASIO legislation by this committee.

Senator PAYNE—Several inquiries.

CHAIR—Several inquiries—and the degree of discomfort that our colleagues viewed us with in relation to our recommendations, which I think reflected concern in the public and concerns raised by the Law Institute, amongst others. Senator Buckland?

Senator BUCKLAND—I just want to raise one issue with you. You talk about privacy and the right of the individual. More and more we are seeing people being arrested without conviction, but we build up a perception of them because the TV and newspaper reporters go to the neighbours, the aunties, the uncles, the mothers, the fathers. How do we protect the people on trial who have been charged but not convicted? This is really going to matters that do not concern the rest of us. There are some high-profile cases around at the moment.

Mr O'Shea—It is not so much an issue of privacy as it is an issue of a right to a fair trial.

Senator BUCKLAND—It does go to privacy because, through the intervention of the media, we are getting into private matters that are not even associated with the crime that has allegedly been committed.

Mr O'Shea—I would agree with that. I do not know whether you can legislate against it. The courts really have jurisdiction over that. It is very difficult, in the age of talkback radio, and indeed with some of the perpetrators of talkback radio, to put too many limits on what they appear to be able to do. The David Hookes case, which affected where I work, was a classic example of where one particular radio journalist took it upon himself to release a large amount of personal information about the person involved, with apparent impunity. I am not sure that any legislation will really affect that. But if it affects court proceedings and criminal

proceedings, courts and judges can deal with it. It gets to the point where a person cannot be tried for an offence because they cannot get a fair trial in the jurisdiction due to that sort of publicity. That has not happened too often in Australia, but it certainly could happen. I think you have to rely on the courts to police that. I am not sure that privacy legislation will really do the job there.

One point worth making about the Privacy Act is that it is very much used as a sword and not as a shield at the moment. We think the act needs more in it—along the lines of what you are saying, in a way—that puts up barriers to information gathering rather than giving people remedies once their privacy is infringed. It is a bit late once your privacy is infringed. It is fine to have provisions in the act that deal with that, but we would like there to be more prohibitions in the act on what can be collected. That is our concern about smart cards, about encryption, about genetic profiling and about the genome information. It is all very well to give an employee a right against an employer who discriminates against them because they have got the genome information. We say that the act should prevent that from happening in the first place.

Senator BUCKLAND—I have great faith in the legal system because I am not a lawyer. I do trust those who are left to make determinations as to a person's guilt or innocence. But I think there is a tendency today for influence from outside. It has got to cloud the issue, surely, if you are on a jury. I have never been on a jury, so I do not know what happens. But you do hear these things and you do look at things the way people are looking at them in the community. It happens more and more, particularly with the high-profile cases. In some of the cases to do with offences against young children, when people are taken into custody we all know who they are. It gets around the streets if it is in a community in which you live. That person is tried by the community. The community now has higher expectations that the outcome will be that those people will be locked away. It is very hard to believe that that sort of influence does not have some bearing on the outcome of a case and that it does not go to matters that are strictly private for an individual.

Mr O'Shea—I think one of the answers is to have a sentencing advisory board, which is what we have in Victoria. Unfortunately, in terms of hit-run accidents, we have seen only this week that, because hit-run accidents have made the media, the Attorney-General has made a statement that we are going to increase the penalty to 10 years. That has not gone to the sentencing advisory committee at all. With respect to the Attorney, it is a knee-jerk reaction to a media report about a spate of hit-run incidents. If you have a sentencing advisory board, as we have here, it can reflect community concern and look at sentences and see that they are appropriate. All you can do is reflect it. We cannot have mob rule. We cannot have vigilantes running the justice system.

Senator BUCKLAND—We cannot, but we tend to be going that way. When I look at New South Wales I sometimes wonder. Not being a legal practitioner, I do not know. I am just guessing.

Mr O'Shea—Judges hear the facts. Judges have to make decisions on what they hear. Sentencing boards can give directions about sentences. The shock jocks who make comments about sentences have not sat through the trial; they have not heard the evidence. A lot of my time as president of the Law Institute was spent dealing with talkback commentators commenting on sentences which appeared to be lenient. But those commentators had not sat through the trial and

they had not heard the evidence. You have to rely on the justice system and the judges to deal with that. If we start moving away from that, we do end up with a justice system that is diminished.

Senator STOTT DESPOJA—You began your remarks by referring to the lack of the so-called right to privacy. Similarly, the Victorian Privacy Commissioner said in his submission that maybe we should consider the notion of enshrining in the Constitution a right to privacy. Is that something that you would support? Is that something you would recommend we pay attention to in our deliberations?

Mr O'Shea—We certainly would. I thought it was only others who gave dorothy dix questions! We certainly would support it. I am not sure that there is community support. As you know, the whole concept of a bill of rights is under discussion in Victoria at the moment. The only way that I can see it getting up is to talk about a fairer Victoria act, which is what we are looking at, rather than a bill of rights, so that it is somewhat modified. Certainly we would support a right to privacy in the Constitution. Given the record of constitutional amendments, I would not be too optimistic about it getting up, but we would support it.

If it were there, at least it would mean that future governments would in some way have a fetter on what they could do in terms of legislating in this area. If the committee were to take on board that concept, we would like an opportunity to make a further submission in regard to that. I was not aware that that was even under consideration. We have made representations to government in the past about the need for a bill of rights. I guess we are at the point now where our focus is on a state bill rather than a federal one.

Senator STOTT DESPOJA—At 10.2 in your submission, which relates to technology and privacy issues—and you have since raised the issues of the human genome and genetic testing—you refer us to the ALRC's quite comprehensive report on genetic privacy. I am just wondering whether you have support for specific recommendations in that report or for the general issue of whether or not we need changes to the Privacy Act to protect genetic privacy and guard against genetic discrimination, which you referred to. Or do you have a preference for a stand-alone piece of legislation that encompasses the things that you are talking about?

The reason I bring that up is that you have talked about not only genetic privacy but also the consequences of that privacy not being protected—that is, discrimination. Do you have a view on how best to protect that? Do you do it with changes to the act that we are dealing with now? Do you have a separate, stand-alone act? Do you feel that there are other recommendations in the ALRC's report that would deal with that?

Mr O'Shea—Our view would be that the act should be able to cover it. It is essentially a privacy issue, we believe. If it came down to a discrimination issue, I suppose there would be an opportunity to include it as a grounds of discrimination in the antidiscrimination legislation we already have. Essentially, in terms of the discussion here, we would not see separate legislation being required on this issue. I do not think the current legislation we have in Australia protects us in this area because I do not think it specifically includes the express prohibitions against it that we are suggesting. It does not necessarily have to be directed at employers or insurers; I think it is a matter of an individual's genetic information being the property of that individual and

therefore it needs their consent before it can be disclosed. That way it is applicable to anyone who wishes to have access to it.

There can be exceptions. As I said, it is a bit difficult to go into those exceptions here, but there will be cases where a particular piece of information might be necessary in order to do a job—for example, to actually be employed in an area. The default position ought to be that that information cannot be used without the consent of the individual, and I think that can be done by amending the existing act.

Senator STOTT DESPOJA—Is the Law Institute of Victoria aware of specific cases of privacy breaches in relation to genetic information or indeed aware of complaints or cases involving genetic discrimination in this state?

Mr O'Shea—I would have to defer to the policy committee on that question.

Senator STOTT DESPOJA—I am happy for you to take that question on notice.

Mr Samararatna—I will take it on notice. I guess when we are looking at genetic information, and in particular at the question you have raised, we need to look at the broader context in relation obviously to technology in general. That is one of the issues that we now face. Technology has in many ways gone well beyond the initial act. Obviously asking about the genetic information is a relevant question. When we look at other areas, such as smart cards or other technologies, we really need to look at what the purpose of that technology is. I raise this cautiously, but in some ways it is like gunpowder: yes, it can be used for fireworks but it may also be used in other things as well.

Technology has got to a stage now where we are able to do many things that we could not do even five or 10 years ago. It is rapidly changing. When we look at technology and how it is being used, there are very simple cases—to put it in a practical sense for the public to understand—where, for example, a medical centre or a GP clinic may put our general information onto an electronic database. There is this push for a more integrative health practice, certainly at most government levels. But there is a lack of education about how that information should be properly managed. I think technology has now got to a stage where we need to be cautious or wary of how it is actually to be used. People may go to see a general practitioner, for example, and that information may be put onto their general electronic file. Other people in the practice may have access to that information. The patients attending that clinic may not be aware of what their privacy rights are. Alternatively, the practitioners within that clinic may not be aware of privacy rights either. We are moving rapidly towards electronic databases in these clinics and we need to look at addressing these issues. There are a number of cases—and I would have to take on notice questions about reviewing these cases in terms of genetic information—where patients have come into integrated clinics and not given their consent to their information being put onto a general file.

Senator STOTT DESPOJA—I take your point. I think that the broad issue of the act keeping pace with technological advances, whatever they may be, is one that we obviously have to address. I would, however, argue for distinctions within those technological advances. I put it to you that genetic information is a special case, as opposed to general health information, which, as we know, is more or less provided for under the privacy regimes in this country. I would argue

that, because we have no specific definition dealing with genetic information and no specific protections on a federal level dealing with genetic privacy, it is a special case. That is why I am curious to know if there are any examples of which you are aware.

Mr O'Shea—I will check that and certainly forward any information to the committee.

Senator STOTT DESPOJA—Thank you.

Mr O'Shea—I will give you an example that illustrates the principle: if genetic information shows that a woman is susceptible to contracting breast cancer, should that be grounds for refusing her private health insurance? Clearly not, in our view. It should be irrelevant; it should not even be known to the insurer. It should only be known to a person that that woman believes ought to know. That should be the position. If there were any suggestion that that sort of information could be used in that way, we believe that would be an abrogation of people's privacy and should never happen.

Senator STOTT DESPOJA—I would say that is a case where there is uncertainty at the moment because of the way that we define medical records and information under the act. That is something that disturbs me greatly.

Mr O'Shea—And what is the flipside? We hear people say, 'We want to make health insurance affordable for all Australians.' That sounds good—it is the commercial argument—but the fact is that you have an erosion of people's rights and a denial to some people of their rights to insurance and privacy. You are really in the hot seat on this issue—it is one of the great challenges of being a legislator. It is all very well for us as lawyers to make comments, but you have the tricky job of balancing that. It is a very big issue that needs a lot of thinking about.

Senator PAYNE—In the institute's submission, under item 6, you make some observations about international comparisons, particularly in relation to the EU Data Protection Working Party, which, as I understand it, reported in March 2001 on some concerns they had about the Australian enactments. What has been the result of that? Are there any trade results, as opposed to implications? What has been the impact?

Mr O'Shea—I am not aware of any impact in respect of that. But one of the subsequent issues is the current push for various free trade agreements in Asia. The standards of data protection in Asia are considerably lower than they are in the EU. One of the consequences of that is that if Australian companies, for example, were to put call centres or other operations into Asian countries, the personal information held in those centres would be subject to standards that are arguably lower than in Australia and vastly lower than in the EU. So there are issues in terms of not only Australia's involvement or Australia's privacy regime vis-a-vis the EU, but also indeed in terms of our Asian trading partners, whom we are now rapidly signing up to these agreements with. I think we need to get our privacy protection regime in order so that there is no downstream problem—for example, for an Australian technology company wishing to do business in Europe and suddenly finding that they do not comply and that therefore the data cannot be transferred.

Senator PAYNE—If they have not suddenly found it in the last four years, when do you expect them to suddenly find it?

Mr O'Shea—I do not think it matters.

Senator PAYNE—I think it does matter. If you arguing that the EU Data Protection Working Party and the European Commission's positions are relevant, then if there are issues with no consequences then it does actually matter. If an argument is put forward to us and there are no consequences, what are we supposed to think? I know the government, for example, does not agree with the observations of the EU Data Protection Working Party; the government made its position quite clear in relation to that and said it did not think the EU Data Protection Working Party understood our laws, which is another matter altogether. But I am concerned about consequences. It keeps being advanced to us as being a serious issue, but I cannot find a consequence.

Mr O'Shea—I am not privy to any submission from business groups in relation to that. I do not know what their view is on it. Our view is that, if the two are not consistent, that is a negative for business. But I cannot give you specific examples of where businesses have run foul of the EU directive.

CHAIR—Could you comment on the state of workplace privacy in this country and whether this committee should be prioritising any initiative on a federal level?

Mr O'Shea—I heard what the previous witness had to say about workplace privacy. The Law Institute would certainly support that. As he mentioned, there is a review in Victoria through the Law Reform Commission at the moment on workplace privacy. We have made a submission. We would certainly welcome workplace privacy coming under the purview of this committee and indeed the Privacy Act. We have limited our comments on workplace privacy to the issues that we have already discussed about genetic profiling. But, if there are issues that you believe would warrant inclusion in the process, we would support that. It is the old federal-state divide again. I think it will happen in Victoria, to the extent that that governs workers in this state. But, if the committee were to believe that that should happen nationally, we would certainly support it.

Senator MASON—You suggested that it might be a good idea to protect privacy, to develop a constitutional right to privacy. One thing I do remember from law school was the shambolic nature of privacy jurisprudence in the United States. Ever since the United States Supreme Court divined the right to privacy—the penumbra rights—within the constitution, the right has been used to deliberate on issues ranging from abortion through to the privacy of homosexual sex. Do you think the courts are the right place to resolve those issues or should it be left with parliament? I usually prefer the latter.

Mr O'Shea—It would depend on how the right to privacy was set up. There are various models for, if you like, bills of rights type legislation. One model would be, for example, where a court does not strike it down but refers it back to the parliament, to the relevant minister, for a review, and leaves it at that. It has no actual right to declare it to be invalid. I think that is one of the issues we are looking at in terms of—

Senator MASON—So you would not necessarily defend the United States' position as the optimum experience?

Mr O'Shea—The United States is not a good model for a bill of rights. The opponents of bills of rights use, as their strongest example, the performance of the US. Anyone putting forward an argument for a bill of rights here would not do that. Furthermore, there have been more infringements of human rights, despite the bill of rights, in America. But I think there are more sophisticated models now for bills of rights. That is certainly one that we are looking at here in Victoria in terms of the right for the elected parliament to enact legislation but to at least have a court give a view on it and ask it to be reviewed, and then leave the political process to take its course.

Senator MASON—What flashed into my mind was Roe v Wade and abortion rights. I think it is fair to say that senators struggle with that issue. It is a difficult political and moral issue. I think that is fair to say. In the United States in the end that very difficult problem was flicked to the Supreme Court to solve. I really think it is parliament's responsibility to solve those issues, ultimately.

Mr O'Shea—In the US, the parliament ultimately has a say on who is on the Supreme Court as well.

CHAIR—Thank you. You have given us a lot of food for thought. As this issue proceeds, hopefully we can factor in your views in a more, to you at least, meaningful way than in previous inquiries.

Ms Kummrow—I would like to ask a general question of the committee.

CHAIR—You would like to ask a question of us?

Ms Kummrow—Yes. I know I am not supposed to. Just in light of Senator Hockey's announcement yesterday in relation to the—

Senator PAYNE—Do not promote him; he is a minister and a member of the lower house.

Ms Kummrow—I apologise. In light of his announcement, what is the committee's reporting time frame? The reason I ask that is that I am conscious of the government's pending majority in the Senate and its ability to introduce legislation. Basically, would it wait for you to hand down your report or do you feel that there is a possibility that this legislation could be on the horizon?

CHAIR—Privacy is an ongoing issue and we are going to report by 30 June, with a bit of luck. Whatever legislation the government introduces in terms of what Minister Hockey is talking about will, I am sure, go through a Senate process after 30 June. I cannot imagine that legislation would be introduced before 30 June.

Ms Kummrow—No, that is just the reporting date.

CHAIR—So it is ongoing scrutiny to the extent that the Senate is keen to do so.

Ms Kummrow—Thank you.

Mr O'Shea—If there are interim reports or whatever that you are going to make or if you need more information, we would be happy to provide that between now and 30 June.

CHAIR—Thank you—and thereafter, I presume.

Mr O'Shea—Indeed.

CHAIR—Senators Mason and Payne will be here after 30 June, so I will act in the best interests of the citizens of the country.

[10.33 a.m.]

KREET, Ms Loretta, Solicitor, Civil Justice (Consumer Protection) Team, Legal Aid Queensland

Evidence was taken via teleconference—

CHAIR—Welcome. You have lodged submission No. 31 with the committee. Do you wish to make any amendments or alterations to that submission?

Ms Kreet—No.

CHAIR—Would you like to make an opening statement?

Ms Kreet—Yes, I would. First, I want to speak to you about the fundamental issues in relation to this inquiry. The protection of an individual's privacy is generally accepted in the Australian community as a basic right, especially in relation to financial privacy. Whilst Legal Aid Queensland in the past has made submissions as to the inadequacy of privacy laws in the context of the lenders who are able to access credit reports and what should or should not be included in credit reports, I do not want to concentrate on that today. I want to concentrate on the critical issue of how consumers can obtain redress where there has been a breach of the current privacy laws.

The fact is that, in our experience, consumers do not have effective redress. As a consequence, privacy laws have very little value without that effective redress. This is particularly so in cases of information held on databases accessed by third parties who use that information in determining whether to provide essential services. I am talking in particular about credit reporting and tenancy databases. Where the information in credit reporting databases is inaccurate, incomplete or misrepresents the facts, the ability of individuals to obtain credit is severely limited. In our experience, it can have the effect of forcing consumers into poverty or severe financial hardship. I will illustrate that in a brief way. If you cannot get a car loan, you cannot get to work. You will not get a car loan if you have a default listing with a mainstream lender. It can also affect your ability to obtain accommodation if you have a default listing or you are in bankruptcy. The second aspect of that is that it can cause severe emotional distress. If you do not have a car and you have children, you cannot get those children to appointments, hospitals and schools. It can cause a degree of difficulty for families.

It can also affect those consumers who have those inaccurate reports in terms of their standing in the community, particularly when access to credit reports has significantly widened in the past few years. Also, it can cause severe financial hardship. What often happens for those who have a blacklist is that it forces those consumers into fringe credit markets where interest rates can be as high as 1,000 per cent per annum, particularly in states where there is no cap on interest rates. Mainstream lenders will not lend money until a default is cleared and sometimes not even then. I just want to illustrate that in a particular way. If you have a housing loan through a bank or mainstream lender but then you have a default on your credit report and want to obtain a housing loan, you might still obtain a housing loan, but it can be at significantly higher interest rates.

Even a four per cent difference in interest rates on a $300,000 loan is a difference of $12,000 in interest per annum.

To demonstrate just how critical it is to have effective redress, I am going to present two very short case studies. The first one relates to a young man's attempts to have a flawed credit report removed. It took two years of direct dealing with the Privacy Commissioner's office to remove it and a total of four years before the complaint was finally resolved. The consequence for this man was that he was unable to obtain a mobile phone contract, which was essential for his employment, and he was unable to refinance a personal loan at cheaper interest rates. The second case study relates to a couple with two children who were unable to obtain a car loan because of a flawed credit report. The husband required the car to get to and from work so that he could support his young family. When the Privacy Commissioner indicated that the complaint would not be investigated for at least a year, the family obtained finance through a fringe lender charging interest, when fees and unnecessary insurance and charges are included, of around 40 per cent per annum. The complaint remains unresolved eight months after the initial complaint was made.

I will briefly tell you what is significant about those two case studies. First, with regard to the similarities, both were relatively complex as they required an investigation into the issues of liability. They were relatively urgent given the effect that a default listing has on a person's ability to obtain a loan or maintain employment. They demonstrate a lack of resources in the Privacy Commissioner's office. They demonstrate a lack of transparency in the process and the denial of justice to consumers. What they also do is place consumers in the position of having to prove that they are innocent of wrongdoing. They demonstrate the difficulties that consumers have in making their own complaint without the assistance of legal representation. They also demonstrate the overall ineffectiveness of the complaints handling process.

The second thing that is significant about those two cases is that the first case study relates to a complaint first raised in 1998 and the second case study relates to a complaint raised with the Privacy Commissioner's office in September 2004. The reason why that is significant is that it appears that nothing has changed in six years. In fact, it could reasonably be argued that matters have got worse in terms of resourcing and complaint handling within the Privacy Commissioner's office. That concludes my opening statement.

CHAIR—Thank you very much.

Senator STOTT DESPOJA—Thank you, Ms Kreet, for those examples. They are quite sad examples in terms of the operation of the Privacy Act. You talked about the issue of resourcing. I note that in your submission you refer to the delay or period of time it takes for cases to be addressed, and you have just given us a couple of examples from 1998 and 2004. You refer to the delay of one year or more between the making of a substantive complaint and its investigation et cetera. Is that standard? Is that the average, or are you talking about exceptions to the rule?

Ms Kreet—I think that shows that the complaint process has blown out. In the first example, the investigation was commenced straightaway. In the second example, there was a standard response that said the office was not investigating complaints; they were only opening cases and

investigating complaints that had been lodged in the previous 12 months. So I would submit that in fact that is a standard response.

Having said that, there was apparently—it was not made known to me as an advocate and it would certainly not have been made known to consumers—a process whereby, if the matter were to cease to have urgency, the Privacy Commissioner's office could investigate the complaint earlier. The problem was that there was no transparency in that process, so we were not aware that there was a policy that some complaints could be investigated earlier. We did not know the basis of that; we did not know what criteria were in place to assess whether or not the matter was urgent.

Senator STOTT DESPOJA—I see. So there seems to be a combination of factors here. I am wondering how much of it is the issue of inclination or understanding and how much of it is the separate issue of resourcing. Do you have a separate comment on the adequacy or lack of resources for the Privacy Commissioner? I am not sure if you have a dollar figure or if it is a broader comment on the resourcing of that position.

Ms Kreet—We do not have an idea of what would be adequate resourcing; all we know is that at the moment there are not enough resources to do the two functions of the Privacy Commissioner's office. One is complaint handling and the other is effective enforcement, because one of the issues is that a systemic problem might exist within the industry but there is also the issue of individual complaint handling. I understand that, in a climate where resources are limited, enforcement should be strategic so that the successful enforcement action changes industry practice. If all the office is capable of doing is handling individual complaints then industry practice will not change, because there does not seem to be effective enforcement across the industry.

I can understand that, when you have the situation of a complainant not being able to get a housing loan because there is an inaccuracy on their credit report—which means that they might lose thousands and thousands of dollars—and they have a very short time frame in which to have that resolved, often less than two weeks, there would be pressure on the Privacy Commissioner's office to deal with that complaint instead of looking at a greater and more strategic enforcement program. I hope that answers your question.

Senator STOTT DESPOJA—It does. I read in your submission the proposals that flow on from that in relation to compensation and apologies. I understand the issue of changing industry practice. I am curious, though, beyond the issue of credit reporting, whether there are other examples you are aware of, or cases that you deal with, where the Privacy Act is seemingly inadequate or whether there are cases that you deal with through Legal Aid that involve a breach of the Privacy Act. There are a range of issues. One area I am interested in is new technologies, including genetic technology, and whether or not you deal with any complaints about those kinds of privacy breaches. I know that is slightly different from credit reporting arrangements, but I am curious whether there is that broader involvement.

Ms Kreet—In a lot of the cases that we have at Legal Aid Queensland, even in relation to breaches of privacy laws and credit reporting, consumers often do not realise that there has been a privacy breach until it affects them directly. They may not be aware that there is a privacy breach in relation to credit reporting, because often they are not told that there has been a default

listing made until they try to obtain credit. So often they do not even know that there is a problem because they are not told about it. It often raises its head as a secondary issue for us so that, when we speak to people who may be having problems repaying a loan or being pursued by a debt collector for a statute-barred debt, we raise the issue with them about whether they have accessed their credit reports recently to see whether that default has been listed inappropriately. So there is an issue about awareness of consumers about how their privacy has been breached. Except for tenancy databases, which I can only speak about briefly, it is not generally the sort of thing that Legal Aid would be getting through our complaints line at the moment.

Senator STOTT DESPOJA—I understand. Thank you.

CHAIR—Ms Kreet, the committee has no further questions. Thank you very much for your submission and for sharing those experiences. One of the critical areas in the legislation is not just the legislation but how it is implemented. Your experiences have been quite useful to us.

[10.55 a.m.]

CLEMENT, Mr Noel, General Manager, Domestic Operations (National Programs), Australian Red Cross

HEESOM, Mr Greg, National Manager, International Humanitarian Law, Australian Red Cross

TICKNER, Mr Robert, Secretary-General (Chief Executive Officer), Australian Red Cross

CHAIR—Welcome. Do you have any comments to make on the capacity in which you appear?

Mr Tickner—I am known as the Secretary-General of Australian Red Cross, but my board takes the view that chief executive is a more appropriate term in the Australian context.

CHAIR—You have lodged submission No. 44 with the committee. Do you wish to make any amendments or alterations, or would you like to start with an opening statement?

Mr Tickner—With your approval, we would like to make some opening comments and then subject ourselves to your questioning. Firstly, we would like to thank you very much for the opportunity to talk to you. We come to this table not as zealots crusading for some change in the law but in a rather considered way, recognising the complexities of the issues that arise from what we put before you and, on behalf of Australian Red Cross, wanting to have some informed discussion about the challenges and the ways in which they might be able to be resolved. While making some opening comments myself, if it is possible I would like my two colleagues to supplement those comments. My colleague Noel Clement has had immediate experience dealing with the aftermath and the victims of the Bali appeal and can assist the committee with that experience. Mr Greg Heesom is our international humanitarian law expert and, since I call myself a refugee from the law, is a much more able exponent of issues arising under the legal principles. Australian Red Cross is very pleased with the fact that we are having a dialogue with the government about some of these issues and working constructively to examine ways in which some of the challenges might be able to be addressed. It is not for me to tell you about those things—it is really a government issue—but that dialogue is useful and constructive and we are very pleased to be a party to it.

I should also say that, if amendments to the privacy legislation were to occur, they may not on their own be the solution to the challenges that are presented, and my colleague Greg Heesom will add to that. There may well be other challenges presented by legislation which establishes other Commonwealth authorities which also have their own constraints on the release of information. While the submission advances the proposal concerning the availability of information to agencies engaged in emergency disaster relief generally, we would also like to use the opportunity of this discussion with you to advance the special considerations that apply to Australian Red Cross as an auxiliary to government, and again my colleagues will supplement that in what they have to say.

The reason why Australian Red Cross put forward the submission was that, first and foremost, the Department of Foreign Affairs and Trade submission, which identified the need for sharing information in emergency situations, is one that we support. We have some variations, but we do support the direction of that submission. We also think that Australian Red Cross has some unique experience arising from the Bali appeal to contribute towards your inquiry. Specifically, we are committed to raising these issues as a result of recommendations in a PricewaterhouseCoopers report that was produced for Australian Red Cross and is available to you in the aftermath of the Bali appeal. I do not know that the terms of that document add substantially to what we are saying, but it is certainly one of the motivating factors that have brought us to the table to give effect to that commitment.

Thirdly, we draw your attention to the fact that the tragedy of Bali may not be—and almost certainly in the course of humanity and future events is unlikely to be—the last time, for one reason or another, that there is an emergency situation that gives rise to similar needs as those that emanated from that tragedy, so we think there is a need to address the issues. Finally, and this refers back to the earlier point that I made, the Australian Red Cross has a unique standing in Australian society, as does the international Red Cross and Red Crescent movement globally. We are formally recognised as an auxiliary to public authorities in public disaster. That auxiliary status is recognised under international instruments and in the ARC's royal charter. In respect of that role, we are able to be distinguished from all other humanitarian actors. The concept of being an auxiliary to public authorities dates back to the origins of the Red Cross and Red Crescent movement, and specifically to the proposals of the founder, Henry Dunant, to assign volunteers to help the medical services of the armed forces. The medical services were, of course, to have the main responsibility for taking care of wounded and sick soldiers on the battlefield while relief societies would be auxiliaries to these medical services.

The statutes of the Red Cross and Red Crescent movement, which have been approved by all the states who are party to the Geneva conventions, refer in article 4(3) to a broader role for a national Red Cross society as 'an auxiliary to the public authorities in the humanitarian field'. In Australia, the royal charter of the Australian Red Cross provides, in paragraph 1, that the primary objects are furnishing of aid to the sick and wounded irrespective of nationality, the rendering of assistance in case of any great public disaster, calamity or need, and the improvement of health, prevention of disease and the mitigation of suffering in Australia or elsewhere. Finally, article 2 provides that the society shall have such powers as are necessary and convenient for carrying out the objects of the society. It goes on, in paragraph 11, to indicate that, without limiting the generality of the foregoing, it shall have power to 'render aid in the event of any great public disaster, calamity or need in Australia or elsewhere'. As I said, my colleague Greg Heesom would be happy to add to that should the committee wish to explore those issues further.

I will conclude my opening remarks by talking very briefly on the impact of the privacy provisions in relation to the Bali appeal—my colleague may wish to supplement, depending on the wishes of the committee. The first major challenge was that the Australian Red Cross was unable to access lists of deceased, injured or missing people, which were held by the Department of Foreign Affairs and Trade. While the ARC worked very closely with DFAT, privacy provisions prevented the sharing of this information. The second challenge was that the ARC was unable to share its own lists of deceased and injured although requested by some state and territory governments which did not have comprehensive lists. In other words, they wanted to provide services to people but did not know who the people were that they were trying to assist.

Thirdly, some victims were registered on the national registration and inquiry system, which is a computerised victim registration and inquiry system operated by the ARC. But, because of the extent of their injuries, they were unable to give the permission to share the information. Finally, the Australian Red Cross needed to seek individual client permission to share even basic information about the assistance provided.

To make that into a more human or concrete example, just imagine, in the aftermath of the disaster that has occurred, someone with horrific injuries who has to tell their story to authorities and to others and who then seeks relief. The person's injuries may range from modest to severe, across a range of possibilities, but, whatever the severity, they have been through a terrible trauma. They have told their story and telling the story just adds to their stress levels. The problem that people found is that they had to tell their story not once, but they had to tell it often to a range of different authorities who might be there to help them for one reason or another. I guess we are here, motivated by concern for the victims, to look for a simplified procedure that does not result in a sweeping away of people's rights to privacy but, in the very limited circumstances of this kind of emergency, provides some practical pathway forward that assists in making people's lives less stressful than it might otherwise be. That is all I have to say. Is there time for my colleagues to add to this briefly, or would you like to move to questions?

CHAIR—There is, but they should do it briefly because we have another witness appearing in about 25 minutes.

Mr Tickner—Good; we will keep it tight.

Mr Clement—Many of the Bali victims and families that we dealt with actually expressed surprise that we did not have access to that information. We undertook a lot of additional work to get in contact with victims, including advertisements in major newspapers. We set up a national 1800 number; we set up a network of caseworkers. We certainly worked as hard as we could to get in contact with people, but people would express surprise that we did not already have that information—particularly in the early stages. In demonstrating people's level of injury, obviously there were some public accountability requirements that we had to demonstrate that people were actually injured and required assistance. Without access to some sort of official list of who had been evacuated or who had been hospitalised, for instance, that meant we had to work with families to get other documentation. It was an added burden at a time when the families probably least needed that additional burden.

Mr Heesom—The only point I would make is that it is clear from the preamble to the act that its creation resulted from the OECD guidelines on privacy. It is probably fair to say, if we look at the second reading speech and the explanatory memoranda, there was no intention to limit the exchange of information in emergency situations such as this, and so you see in the IPPs—in IPP 11, in particular—provisions for disclosure include statements like 'Would the individual concerned be reasonably likely to be aware that information would be passed on'. In situations such as Bali or other emergencies that we have seen where we have been the major appeal organisation, and it is clear to the public that we are providing assistance to victims, is it reasonably likely they would be aware that information should be disclosed so we can provide that assistance? It is an issue of interpretation, but I do not think the original drafters would have suggested that it should be restricted in those circumstances.

There is a range of other disclosure provisions that might also apply here, but in limited circumstances. The difficulty is obviously in the interpretation of that by each agency, and agencies may or may not err on the side of caution. There is a significant issue there. I also want to add briefly to the point that Mr Tickner raised: resolving the issue here is not the only issue. As I am sure you aware, a number of other agencies have limitations on their ability to disclose information. They have security provisions which limit that but that also pass on that security restriction to agencies who receive the information. There will be a need for the committee to look more broadly at those issues as well.

CHAIR—I will start by trying to be specific on this particular issue, because I think it is going to be one of those issues that has to be addressed by the parliament. I am wondering what the best way to handle it is. I understand that privacy principles apply. What you try to get is a waiver when there is an emergency situation or when a person is not capable of waiving their rights to protection. I wonder whether the issue could be tackled by going to the second scenario I mentioned or whether there needs to be an exemption in cases of crisis situations, emergency situations. Can you address that part first?

Mr Heesom—While ever it remains an issue of interpretation, there will be problems. I think there are two solutions that could be advanced. One is a public interest determination by the Privacy Commissioner, but again that will leave the issue open to interpretation as to whether, in a particular scenario, that public interest determination would apply. I think the issue also is that government legal officers in each agency will need to assess their own legislation, the privacy legislation and the public interest determination and determine whether it applies in that circumstance. So I think there is a difficulty either leaving it just to broad interpretation or a public interest determination. A specific exemption under IPP 11 I think provides clear guidance and is perhaps the best solution, though, as Robert indicated at the start of the session, we are not privacy experts and do not profess to be. Certainly that appears to me to be the avenue that would provide for the best response in a time of crisis.

CHAIR—I wonder whether you can help us. You say you are not privacy experts, and I understand you may not be able to give this answer, but what happens normally in a situation where someone is not capable of waiving their rights? Is there provision in the act?

Mr Heesom—IPP 11(1)(c) is an exemption that allows for disclosure in limited circumstances, and that is to prevent a serious and imminent threat to life or health. Again, that can be interpreted very narrowly if you interpret the terms 'threat' and 'imminent' in a particular way. Equally, you could define 'threat to health' broadly in the sense of whether a person needs psychological counselling as a result of the trauma they have either experienced or witnessed. So, yes, there are other exemptions. There are also exemptions in relation to criminal law and in relation to the protection of public revenue, but all the exemptions apply in limited circumstances, so we do not have anything that specifically targets this issue.

CHAIR—But if we, for instance, were to recommend a course where, in cases of national or international emergency, parts of the act be waived, we would have to go down the road of defining what those emergencies are, the extent of the waiver, the obligations on NGOs and what sort of NGOs. They raise a lot of issues as well. For instance, from your experience with Bali and with more recent affairs, would it be easier, in a situation where a person is concussed or whatever and incapable of waiving their rights, to have a provision in the legislation that would

allow for that, or do you think a broader provision for the whole emergency would be more appropriate?

Mr Heesom—I think you have in 11(1)(c) that limited disclosure for the situation that you are talking about. I might refer back to Noel.

Mr Clement—In the Bali situation, there were a small number of people who had been concussed or who were unconscious and in a coma. They were largely people who were medically evacuated. So that certainly would have dealt with a small number of people. The majority of people in the Bali situation did not go through a process with Foreign Affairs where they registered their information, and they were not asked, 'Would you like this shared with other recovery agencies?' because that information was already on the public record. I particularly remember speaking to one family member. Because this was such a large national emergency, governments were providing assistance and we were clearly working hand in hand with government—we did a lot of work that was complementary to government assistance—she just expected that we would write to her or make direct contact with her. She expressed concern that that did not actually happen.

Mr Tickner—In other words, while the point that the chairman raises is certainly an important issue, it is not the only one.

Mr Clement—A national registration inquiry system would potentially deal with that situation, where you registered people who were unconscious instead of going to default. The default at the moment is to not release information unless someone specifically waives that.

CHAIR—What was the actual problem—that you could not tell relatives, that you could not help identify people or both?

Mr Clement—It was that we could not identify people to target assistance to them. You had people who were in hospital and family members from all around the country travelling to be with them. They did not necessarily have time to go and seek out assistance, so it meant that we were going to hospitals and making direct contact with people. We were using all sorts of unconventional means to let people know that assistance was available. We actually had to reach out. I guess the issue is that we cannot expect people to find us, and their expectation clearly was that we would find them.

Mr Heesom—I think it is important to bear in mind also that, if you provide for a disclosure in the information provider's privacy principles, the protections otherwise would still apply. Certainly as an agency we would still be required to comply with the privacy principles in how we subsequently collect, use and disclose information. It is not that once it is released that information is then available. We are still restricted by the national privacy principles—

CHAIR—Not if you waive them all. If you are talking about limited waiver, then fair enough. But if you are talking about waiving the operation of the act then we have to find some way of making those principles apply.

Mr Heesom—One of the suggestions is not to waive the act but to allow disclosure in limited circumstances, but when you disclosed that information you would still be restricted in how you

used it. Were we able to access the information, we could only use it for the purpose for which it was disclosed. It would be limited to us providing the assistance that we have been asked by the Australian community to provide.

Senator STOTT DESPOJA—Thank you for clarifying that, Mr Heesom. I would be very wary of talking about a waiver provision in relation to the act because of the issue that you have just raised—that is, the consequent dealing with the information that has been obtained. I think you may have also answered my other question. I was trying to work out the extent to which you were precluded from gaining information, given that under principle 11, as you have referred to, there are grounds on which I would have thought you might be able to access information.

Let me go back a step. In your submission—and Mr Tickner has made comments today reinforcing this—you say that you were unable to access information from DFAT, for example. Your submission says:

Privacy provisions prevented sharing of this information.

I would like to break that down a little as to how, exactly. I am wondering, depending on the nature of the information DFAT obtained and how they obtained it, whether or not they were in a position, in some circumstances, to get a consent, an authority to disclose information to you and other agencies—depending, obviously, on the nature of that information. When you talk about it being almost like a brick wall, what were you asking for and what did you not get? A list of the deceased? A list of the injured? A list of their families? A list of what they want?

Mr Tickner—That is a good question. I think Mr Clement can help with this one.

Mr Clement—It was initially a list of the deceased and the people who had been medically evacuated or were listed as missing or injured so that when families approached us we could identify whether their son or daughter was clearly an affected person. In terms of accountability we could have skipped through a whole lot of necessary documentation if we had access to that information. It also meant that we could make direct contact with people if we were able to. The information DFAT collected, as I understand it and I am not from there obviously, was partly through their inquiry centres. They would have people ringing up and inquiring about somebody who was overseas and DFAT would have access to lists of people who were in Bali at the time and were able to do some matching in identifying, from the inquiries that families were making and the lists they had, who was actually a person of concern as a result of Bali. It was not just DFAT; families registered with Centrelink, the Health Insurance Commission and a number of other agencies to get certain types of assistance. I have to say apart from DFAT though—with Centrelink and the Health Insurance Commission—within those first few months, I think Australian Red Cross probably had more of those families registered and our information could have been as much use to those agencies as the other way around.

Senator STOTT DESPOJA—I am trying to work out a way in which you do not have to insert waivers; I can understand there may be an issue for exemptions. My preference is always to specify the circumstance as much as you can in the act to make sure, of course, that it is not abused in any way—and that is not a reflection on Red Cross. I am wondering whether this is something that needs to be discussed with an agency like DFAT, and maybe we are not looking at legislative change in the context of the Privacy Act but a way to ask for consent and vice

versa. I am trying to work through it all and am wondering to what extent the privacy provisions actually prevent the sharing of information. Within the privacy principles and within the act there are, as you know, opportunities for the sharing of information, but a lot of that relates to consent and authority. I am wondering whether section (C) to which you refer, Mr Heesom, might be amended in a way to cover this without more substantive change.

Mr Heesom—There are a number of ways that the issue could be resolved, but my view is that they would not resolve the issue sufficiently. For example, when DFAT collects information it could advise the people it is collecting information from that it will be disclosed to agencies providing disaster relief services. When you collect information, you can always advise the person of your disclosure practices, so that is an option. But the issue in that situation will be: is it always going to be DFAT? It may be DFAT most of the time in an international situation, but it potentially may not be DFAT in a national disaster. It may be that a state agency or a collection of state and federal agencies are involved. How do you ensure that everybody, whoever is involved, is aware that when they collect that information they need to ensure that the people are informed that it may be disclosed? That is one option but, as you can imagine, there would be gaps in that; it would not always work. Yes, IPP 11(1)(C) could be modified perhaps to refer to emergency disaster situations or situations where there is a serious or imminent threat to life or health.

Mr Tickner—The point needs to be made that we are talking about a pretty extraordinary circumstance of a major disaster. Whatever the path through this that is ultimately taken by the wisdom of the committee and/or the government, the problem we are trying to solve is the significant disaster and the chaos and trauma that that sort of situation brings about. So I emphasise that that limited area is our concern.

Senator STOTT DESPOJA—I understand that. I do not think we are going to solve this in questioning today, but I see that you have PricewaterhouseCoopers' report and their broad recommendation for dealing with this issue. I am wondering whether they or you have any more specific recommendations, and I am happy to take that on notice. Also have you brought this to the attention of any other government authorities, legislatures or even the Privacy Commissioner? I suspect a way forward might be through looking at the work done to date where people have, oddly enough, envisaged some of these circumstances, but you may feel they are not provided for within the act as it currently stands.

Finally, are there any specific legislative changes that you have come up with? I gather from the submission and the discussion today that, apart from one section of the act, you do not have a form of words or perhaps any international comparisons that you could offer. I thought that looking at comparable privacy legislation might be the next thing that we would do. That could include legislation in those countries that were obviously affected in recent times by disasters. I presume we are going to have to, and I would like to, pursue this further, but it would be nice if you could give us more information as to what work you have done on this to date.

CHAIR—You might want to take some of that question on notice.

Senator STOTT DESPOJA—I am happy for you to take that on notice if you prefer.

Mr Clement—I can certainly respond to how the PricewaterhouseCoopers report dealt with it. The report does not go into that level of detail as it was not the primary purpose of the report. The report was about issues surrounding the Bali appeal and privacy was one issue that they noted in talking to people such as me and our caseworkers. It was about the amount of work that was required in that early stage and any perception that this may have led to some delay in providing assistance. Their finding was actually that there were no delays in providing assistance but that the privacy laws did not help the situation and meant that there was that added burden on families and certainly on the organisation to work around them.

Mr Tickner—I will add one other thing. It is just for information, but I guess it is relevant to this broad questioning. I am very pleased and proud to say that Australian Red Cross, with the support of some government backing, is a major actor in the International Federation of Red Cross and Red Crescent Societies in advancing concepts around international disaster response law. Significant projects are being undertaken in Geneva, and the Australian Red Cross is very grateful for the government support on that, because it raises some bigger-picture issues that the world needs to come to grips with. You may also be interested to know that the primary actor and researcher is—and I am quite happy to say the name—Victoria Bannon. So there is some very interesting pioneering work, with the support of the government, happening from a South Australian point of view. It is good to know that is happening.

Mr Heesom—We will undertake to follow up with Geneva because they have just conducted the initial worldwide study to see if privacy issues were raised there and see if they can provide the information.

Mr Clement—We can also follow up specifically with the American Red Cross and the Spanish Red Cross, who both responded to 9-11 and the Madrid bombings respectively.

Senator PAYNE—Mr Tickner, in your opening remarks you indicated that the Australian Red Cross was in a dialogue in government and that you did not wish to go to the detail of that. We understand that completely, but could you indicate to the committee with which part of government you are in dialogue?

Mr Tickner—My colleagues were both present at a meeting yesterday and we sought guidance. We are not trying to pre-empt what others might say, but essentially a number of agencies have come together and are examining these kinds of questions. My colleague Noel Clement, who was there yesterday, might go as far as we are able to go with this.

Mr Clement—We have worked with a number of agencies on recovery task forces around Bali and the tsunami. Those are agencies such as foreign affairs, Family and Community Services and health. All of the major players in disaster response and recovery have been involved in those discussions. It has come up in many forums. It has come up in debriefs around both Bali and the tsunami. We have been involved in many discussions around it and I know that it is an issue that those agencies have all identified as one that they want to try and find solutions to.

Senator PAYNE—I wanted to pursue very briefly some of the observations that Senator Stott Despoja was making about how best to address this issue. I appreciate the difficulty in which it places your organisation and the difficulty in which government agencies find themselves. I

think you said that people were surprised at the lack of access that the ARC had to information. I suspect, though, that in an equal number of circumstances people would be surprised if the ARC did have access to that level of perhaps personal information in some of these circumstances. It really is a very difficult line to walk.

Mr Tickner—Perhaps I could ask Mr Clement to respond to this. He is the one who was there at that front line for us. Noel, please just tell the committee honestly about your experiences with what victims and their families wanted from us.

Mr Clement—We made contact with families through other means, often through public advertisements, word of mouth and other family members. Certainly, it was reported back to us that there was more surprise that we were not making direct contact with them and did not have access to that information. I do not recall any situations where we contacted families and they were surprised that we had been able to contact them. Further down the track that may have been different, but in that first emergency phase I am not aware of situations where families did not want to be contacted. There were certainly people who said: 'I'm not ready now. Thank you for the information. I'll come back later.' And we certainly respected that.

Senator PAYNE—The observation that one of our witnesses made—I am not sure which of you it was—was that, at the time to which you are referring, it was a particularly fraught, difficult, frenetic, tragic environment. People's capacity to make decisions and to be aware of what is possible and permissible and what is not is not necessarily at its peak either. You are dealing with people in a time of great stress and strain.

Mr Clement—Absolutely, and you are dealing with family members who may have travelled across the country to be in a hospital next to somebody who is very unwell. We were providing assistance with accommodation, transport and a lot of those things that they may not have otherwise been able to cover themselves. They were very appreciative of that support, but, quite understandably, they would have preferred not to deal with any of the documentation and things that might have been required around the provisions of that support. In addition, a lot of family members were not at home, so contacting them was quite difficult.

Senator PAYNE—It gives us something to think about.

Senator MASON—Gentlemen, my more pragmatic colleagues have asked about legal process. I might ask a perhaps impertinent question about principle. On page 2 of your submission, under the heading 'Information Sharing by Agencies in Emergency Situations', you say:

> ARC contends that, in emergency situations, there is a need for provisions that enable sharing of information across agencies engaged in the emergency response ...

I understand why, but this committee frequently hears from other agencies that they need further information in times of emergency and great stress. For example, the Australian Federal Police say they need further information in times of national emergency—that there is a ticking time bomb and we need to be able to cut through the privacy laws so we can do the right thing. I am sure you are trying to do the right thing as well, but what we are all concerned about is the consistent erosion of privacy rights. Here again you are asking for privacy rights to be

diminished. I am not saying it is not a worthwhile cause, but if Mr Keelty were sitting right there he would say, 'We need these powers as well to do good by the Australian people.' How do you respond to that? Why are humanitarian concerns more important than law enforcement concerns in an emergency situation?

Mr Tickner—I guess I would respond to it by respectfully declining to become involved in a wider discussion, because I truly believe that that is a matter for the parliament and, in this case, the committee to weigh up. There are very great challenges—we certainly would agree with that—but I do not think we would want to buy into that wider public debate. Our submission is limited because we are very focused in this area.

Whilst it can be argued that there is a lessening of privacy rights, our first point is that the lessening of privacy rights is extremely limited, as we have been stressing in the course of our submission. We are not opening a Pandora's box here: we are not asking for anything other than very basic information, and in the very limited circumstances of this kind of emergency disaster situation. We believe that if the information is given then the use to which it can be put needs to be dramatically constrained in the way that I think all the senators have implicitly suggested.

Senator MASON—Sorry to interrupt. As Senator Stott Despoja, Senator Bolkus and Senator Payne have illustrated, if it is an emergency situation the Australian Federal Police are very useful and, I think we would all agree, perform extremely well in these contexts. As to the merging of an emergency role by the Australian Federal Police in terms of setting up morgues and these horrible sorts of things, with their law enforcement role and the diminution of privacy rights, there is an issue. It is quite difficult to draft legislation where, in a certain emergency context, the ARC may be allowed access to certain information but not the Federal Police. I think our concern is that agencies working together can have access to information. When you say they cannot use it for other purposes, if the Australian Federal Police have the information, they will use it.

Mr Tickner—I appreciate the way in which you are mounting the argument, but you would appreciate that the Australian Red Cross would not want to buy into a wider debate. It is just not what we do. I do hear you but, respectfully, it is not where we would want to go. I make the point that, while it could be quite obviously argued that what we are proposing is a reduction or a change in the privacy legislation to allow the flow of information, we believe it is incredibly narrowly constrained. Once the information is released we also believe that what could be done with it should also be very dramatically constrained. We do acknowledge that these are very difficult issues to balance. The sentiment that you have expressed is one that is understood and respected by us. It is a very difficult thing to weigh up. I guess what we would say though is that there is another side to the equation—that is, the benefits in this particular case that the victims and their families would have. That is the challenge to weigh up. That is all we would say.

Senator MASON—You have put your finger on it. It is so sensitive. The other day when I was in Brisbane I saw an article on the front page of the *Australian* from Wednesday, 20 April titled, 'Privacy laws stopping police acting on travelling paedophiles'. The argument is that privacy laws were stopping the exchange of information, so paedophiles were going overseas and potentially engaging in paedophile activity. In a sense, if you are a privacy advocate, you are saying, 'These privacy laws must remain.' Of course the argument is that you are protecting paedophiles. It is a very difficult political balance to strike. I noticed the next day a spokesman

for the Australian Federal Police—I think it was Mr Keelty—saying, 'We are not even alluding to the privacy laws; we are simply tracking paedophiles irrespective of the privacy laws.' I am not sure that that is a good thing or a bad thing. The point is that it is such a difficult political balance.

Mr Tickner—I am living proof to all of you that there is life after parliament. I can tell you that there is not a day that I wake up when I am not pleased to be in my current role. In that current role I have to say that, respectfully, that is not an area that I would want to go to. The Australian Red Cross is not able to and does not wish to participate in that debate. That is my honest answer. I really have nothing to add. I do hear what you say.

Senator BUCKLAND—There is only one more question; you have actually answered it.

CHAIR—Then we can move on.

Senator BUCKLAND—I will continue to ask it. As far as privacy is concerned in cases of humanitarian activity, such as the Red Cross and like organisations, you are not looking for information that goes beyond the immediate next of kin or medical records, are you? So drafting regulations would not be as difficult as it might be if you were going to give those same rights to, for example, the Federal Police?

Mr Tickner—Thank you for that question. Yes, it is very narrowly constrained. Greg is probably the most appropriate person to answer that question.

Mr Heesom—I think Mr Clement mentioned this, as does our submission. At a minimum, we were looking for the details of the deceased and the people affected so that we could simply contact them or their families and indicate that the Australian public had donated a significant amount of money to assist the victims, that assistance was available to them and, if they need it, they should contact us. That was essentially it.

Mr Tickner—As simple as that.

Mr Heesom—We are not looking for more detailed records. Equally, I take Robert's view that we do not want to engage in the political debate, but we are not looking at the data matching issues that perhaps have often been an issue in this privacy debate between different agencies—collecting information for one purpose but then data matching and using it for another. We are not looking at that sort of issue at all. The information we sought was to let people know that assistance was available. Essentially that was it.

Senator BUCKLAND—I have questions that arise out of that. It is something that you probably cannot answer now but you might take it on notice. In relation to the drafting of such regulations to provide this information for you, has the ARC turned its mind to drafting anything along those lines?

Mr Tickner—We have not, but we will investigate what is available internationally. It is not something we have done yet.

Mr Heesom—I would have to say that I think drafting is best left to parliamentary counsel. I think it is fraught with difficulty.

Senator BUCKLAND—Sometimes the first draft helps the second draft develop, doesn't it?

Mr Heesom—Yes, certainly. As Robert mentioned, we will undertake to see what information is available from the international study conducted by the federation.

CHAIR—Thank you for your submission. Without going into a big debate, I think Senator Mason's point is still a pertinent one. If you create an exemption precedent for one situation then there will be demands for others, so we need to keep that in mind. Thank you.

[11.43 a.m.]

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

CHAIR—Welcome. You have lodged a pretty extensive and valuable submission, No. 17, with the committee. We have not published it as yet because there is one aspect of it that provides adverse comment with respect to another organisation. As a committee, we have decided to publish your submission and the response from Hitwise and not address those issues this morning. If you would like to come back to us with respect to Hitwise's response then you could do so in writing. Before we publish anything further from you, we will make sure that they also have a chance to reply at the same time. With your submission this morning, if you could go to everything other than that particular adverse comment, we can proceed. Do you wish to make any amendments for alterations to your submission?

Ms Graham—No, thank you.

CHAIR—Would you like to start with an opening comment?

Ms Graham—Yes, please. Firstly, I would like to make just one short comment about the publication of our submission. I believe there has been some indication that EFA has already published that submission. I would like to make it clear to the committee that EFA has not published or made available our submission to anybody other than this committee. In terms of an opening statement, as our submission said, we are of the view that the current legislative regime does not adequately protect the privacy of Australians in relation to technologies that have been in use for a decade, so we certainly do not believe that it has the capacity to respond adequately to new and emerging technologies.

One aspect of the existing law that we feel creates a large part of the problem is that there is no effective prohibition on the collection of personal information in the first place. The national privacy principles in relation to business organisations do not restrict collection, provided that the business can claim that it is necessary that they collect that information for one of their functions or activities. We therefore have a situation whereby basically an organisation can set up an extremely privacy-invasive business model and then claim that it is necessary for them to invade people's privacy in order to be in business. They would be allowed to do that because NPP1 allows them to collect information that is necessary for one of their functions. We believe there really ought to be some stronger limitation on the collection of personal information where it is not just up to a business to claim that something is necessary and where arguably the individuals do not want the organisation to be providing such functions in the first place.

We also are very concerned about the current definition of personal information, and we have also raised this in our submission. With new technologies, particularly in the area of telecommunications—it is already occurring in relation to biometrics and so forth—there are a huge number of questions about what the definition of 'personal information' actually means. It refers to information from which a person's identity can be reasonably ascertained. Over the years to date it has been generally accepted that information like a street address or a person's telephone number is arguably personal information because you can identify individuals from

their street address or their phone number. Now, particularly in the internet space, we have a situation where individuals using their laptops or their computers at home are having IP addresses allocated to their computers.

Some people will argue that an IP address is not personal information because it identifies a computer. But in our view it is exactly the same as a phone number or a street address. Because there may be only one person using that particular computer—there may only be one person that logs on to the ISP with that IP address—to us it clearly does in some instances identify individuals. Increasingly, with the greater prevalence of ADSL services it is far more common to have a static IP address—that is, the same IP address every day when you have an ADSL connection as opposed to when you have a dial-up internet connection.

With the older style, dial-up, where each day you had to dial a phone number to log into your ISP, you would certainly get a different IP number every day. But now, with ADSL, you have an internet connection which is always on and you can have an IP address that is almost permanent or it may be the same number for several months. With my ISP, for example, and my ADSL connection, I find my IP address does not change for up to six or seven weeks. So certainly anything you have done that has tracked your IP address over that period of time can be data matched back to you or, at the very least, one or two other people who may use the same computer.

It is also pertinent to note, in terms of whether IP addresses should be regarded as personal information under the law, that the IP address is the main thing that law enforcement authorities use when they are trying to identify criminals. For example, under much of the cybercrime legislation, where they are trying to find hackers and so forth, it is the IP address that the police will be getting from the web site that was hacked or whatever to then track back through the ISP to find out who was using that IP address at the time.

It is the same where threatening emails have been sent. It will be the IP address out of the email message that the police will be using. We certainly feel that if IP addresses are what the police use to identify criminals then plainly the police must think that IP addresses are personal information and so the Privacy Act should clearly ensure that IP addresses are included as personal information.

We have also mentioned in our submission our concerns about inconsistencies between the Telecommunications Act 1997 and the Privacy Act. We feel that the way the Privacy Act was introduced in 2000 did not look closely enough, probably completely unintentionally, at where there were variances between those two laws. We feel that there needs now to be some amendments made to the Telecommunications Act to make it consistent with the Privacy Act or, alternatively, amendments made to the Privacy Act to make it clear that the Telecommunications Act does not override the Privacy Act. There is just an imbalance there with some of the provisions.

Other matters that we have raised are around smart cards being used for Medicare, drivers licences and RFID technologies in passports. We are very concerned that the existing act does not adequately cover privacy in those areas, again because there are going to be questions of what is personal information and whether the actual technology being used has sufficient security in it so that it is not going to enable anybody in possession of the smart card to access

people's personal information that is on it or access the database where back-up material is being stored. We have numerous concerns about individual privacy principles, the National Privacy Principles. I will not go into those principles again; we have already discussed them in the submission.

The final point I would like to make is that we are also of the view that there really need to be increased enforcement mechanisms and increased powers for the Privacy Commissioner, which also require increased funding. In our view the federal Privacy Commissioner is underresourced and underfunded, and that needs to be addressed before the existing legislation can even be seen to be doing the job that the parliament anticipated in the first place. With regard to the commissioner's ability to cope with the level of complaints, I and two other individuals lodged a complaint with the Privacy Commissioner's office 20 months ago. I grant that it is not the simplest complaint that the commissioner's office would have ever received on the matter of the Privacy Act, but clearly I am alleging that my privacy has been invaded in contravention of the act for 20 months and I am still waiting for a decision from the commissioner. I believe that this is not directly the fault of the commissioner. I do believe that there is insufficient funding and staffing and that these kinds of complaints that are not completely simple are just going to constantly be put on a backburner in the hope that eventually more time or more resources will be able to deal with them. In the meantime individuals who believe their privacy is being unlawfully invaded cannot get a resolution.

Senator PAYNE—Thank you very much for your submission. If your complaint to the Privacy Commissioner reflects the complexity of your submission I am not at all surprised you have not heard back from them. We are doing our best to deal with your submission. One of the questions that I wanted to pursue with you has been in the back of my mind for some time, and this inquiry brings it serendipitously to the front. It is the process for parliamentary scrutiny of government activity in this area in particular. For example, you have raised in part 4 of your submission the smart card technology, particularly in relation to Medicare at the Commonwealth level—'possibilities of function creep', I think you describe it as. You talk about the use of radiofrequency identification chips, particularly in the passport context, the potential for the development of the online national ID document verification service and so on.

Although this committee has some corporate history—it might be stretching the imagination to say 'corporate knowledge'—on privacy issues, there is not really a holistic or comprehensive approach to dealing with the development of technology through government and its application to the community at the parliamentary scrutiny level. As you have identified, for example, the Medicare smartcard was probably considered, if it was considered at all, through a community services committee such as the Senate Community Affairs Committee, or something like that. The passports control initiative was not considered, to the best of my recollection, by the Senate Foreign Affairs, Defence and Trade Committee. We occasionally have other issues to examine, as you are aware, in TI in particular. One area that this committee might be able to contemplate is how best to address that. Initiatives are really being taken very broadly across government, and I do not think there is a holistic appreciation of that. From your perspective, would that be a fair assessment?

Ms Graham—I believe it is. That is very much our concern as well. I think I am getting to the same aspect that you are referring to. On the one hand we have privacy legislation which is fairly complicated to understand. The NPPs are quite difficult to interpret in some areas. Whilst the

parliament is obviously aware of the privacy legislation, it is not necessarily easy to look at it and then look at whether some other initiative is going to be compatible with it. In our view, in recent years a lot of legislation has been going through parliament far too fast, even before organisations like EFA have had the opportunity to properly look at it and perhaps bring concerns to the attention of our local representatives or whoever. We also have a concern that the parliament as a whole always seems to be having to do things at a fairly quick speed, particularly when legislation gets referred to committees. We are seeing committees being given 48 hours or one week to review and report on legislation.

Senator PAYNE—I am familiar with the problem.

Ms Graham—Yes. I was not going to say 'relative to your committee', but, yes, certainly, I was referring to that. To us, it demonstrates the problem that, where you have complex issues with not only trying to protect privacy but also trying to achieve legitimate outcomes in terms of the provision of government services or law enforcement matters, there is not really sufficient time for anybody to look at it properly and to determine whether this is an appropriate balance or how it could be done better. We ourselves do not have a solution to it, other than to say that perhaps there does need to be a committee with a more prominent mandate to look at privacy issues.

Apart from that, our view is that—from the government point of view, as distinct from the parliament point of view—it would be preferable if more draft legislation was being put out for public consultation before it even gets tabled in the parliament. Just as one example of why I make that comment, last year there were amendments to the Criminal Code relative to telecommunications, which a part of this committee would be familiar with. Whilst EFA was not fully happy with the final outcome on that particular bill, the fact that it had been put out for public comment by the Attorney-General's Department very early in the piece did result in a considerable amount of good amendments, without affecting the overall intent of the legislation. Good amendments were made by the Attorney-General's Department before it even got to the committee stage. If I recall correctly, that public discussion period was something like six weeks or two months. It was even longer than what often committees get to look at things. EFA's view is that it would be probably helpful if more complex legislation was open to public discussion before it was even put in the parliament.

Senator PAYNE—I think this committee in its legislative capacity is consistent in supporting comprehensive consultation by the Attorney-General's Department on legislation, no matter what area it pertains to. One of the problems that we have as parliamentarians, broadly speaking, is that we tend to work in silos; it is just the way it works. But across the broad it is difficult for everyone sitting in a caucus or a party room or whatever to have a comprehensive grasp of what is going on in the Health portfolio or in the Foreign Affairs portfolio.

My colleague Senator Mason just alluded to the concept of a privacy impact statement, which has been raised before today. I was not sure whether you had specifically referred to that in your submission.

Ms Graham—I do not think we did.

Senator PAYNE—I was going through your executive summary to see whether you had referred to it, but I do not think you did. Do you have a view?

Ms Graham—Yes. We would support a privacy impact assessment being done on legislation that has the potential to impact on privacy. Probably the reason we did not mention it is that we already had a great deal else to say and time was running out.

Senator PAYNE—Indeed, you did.

Ms Graham—In regard to a privacy impact assessment, the question is: who would be doing it and how would it be done?

Senator PAYNE—We rely on information that comes from departments to tell us what the privacy implications or impacts are likely to be of particular initiatives. If they are also doing their own privacy impact statement—for example, the passports issue was very interesting. I recall the discussion; I do not recall it extending to that depth.

Ms Graham—I do not think it did. I think there may have been an opportunity at some stage for some public comments to be put forward, possibly to the Attorney-General's Department. I just cannot remember the detail. I know we were involved in commenting on some other legislation at that time. We were not active on the passports bill at the time it was in parliament.

Whilst you may have a government department who say, 'We have done a privacy impact assessment,' the question is: who within the department did it, or who did the department contract to do the privacy impact assessment? Did they consult with people concerned about privacy issues or did they just look at it from their perception of privacy and think that this is all okay? As we have said in relation to RFID, it is not just the philosophical privacy issue, it is the question of whether the technology can produce what it is claimed it is going to be able to produce and whether the security is as good as it is claimed it is going to be, and that impacts on privacy.

Senator PAYNE—That is where we are going with it.

Ms Graham—If the government thinks it has this you-beaut piece of technology that is going to protect privacy but the claims about the technology are wrong, obviously we have got the wrong outcome. But it is not even necessarily the government's fault, because the government and the parliament may have legitimately believed that this technology will achieve what it is claimed to achieve. So it is probably not just a privacy impact assessment; it is probably a privacy and security impact assessment—security in terms of the technology. It is not security in terms of law enforcement but more in terms of the actual technical issues.

Senator PAYNE—Yes, I understand that, and that is where we are very limited. As an earlier submission today described us, we are by the nature of what we do generalists overwhelmingly. If somebody tells us from a position of authority and experience and so on what the technology and security implications are, unless we can actually walk behind that—which is hard to do—we do not necessarily end up with a particularly helpful answer. We could then say: 'This is a good job for the Privacy Commissioner. Let the Privacy Commissioner do privacy and security impact

statements.' My understanding from your submission and other submissions is that, under current resourcing, that would simply be a challenge they would be unable to meet.

Ms Graham—I believe that would be quite right and I believe that is what the former commissioner has said. It is not just us who are saying that they are underfunded; the former commissioner has said that in Senate estimates and so forth. My understanding from the current commissioner is that, as she has been going around the country doing consultations, she has commented that she is hopeful that the ways and means will be found of getting increased resources and funding. But it is not evident where that is going to come from yet. So there is definitely an issue with resourcing and funding. It is not just the privacy advocates that are saying this. The commissioners themselves have said it.

Senator PAYNE—Perhaps you might give some thought to: if not the Privacy Commissioner then who?

Ms Graham—Yes.

Senator STOTT DESPOJA—In your submission, when you refer to the smart card, I think you made it very clear that you believe the roll-out of such a card should be halted or should at least be contingent upon a couple of things happening. I think you do actually refer to an independent privacy impact assessment as well as a security impact assessment. Does that mean in principle you are not opposed to the idea of a smart card, provided that personal information is securely protected?

Ms Graham—EFA's position in general is not to actually oppose the technology but to oppose particular uses of it. Our position with things like these Medicare smart cards is that we do not necessarily oppose the use of the smart card, but we would like to see evidence that there is a reason to use a smart card and there is no potentially less privacy invasive method of achieving the same objective. Our core concern with the Medicare smart card proposal at the moment is that there is simply no information at all that explains why a smart card is needed or how it is going to be used to protect privacy and security of people's information. All indications to us at the moment are that it is basically going to have completely the opposite effect. So that is really why we are saying that, at the moment, we think the Medicare smart card roll-out should be halted until there has been a proper assessment of and justification for it. We are not saying that a smart card should never be used, but the question is why it is to be used in any particular instance and especially in this instance. We just do not see how it will have the benefits that it is supposedly being claimed it will have. Just from a technological perspective at the moment, it just does not make sense to us. There is too little information being made available.

Senator STOTT DESPOJA—I note your comments in your submission about public consultation. I am assuming that public consultation would not be restricted to, say, a Senate or comparable inquiry.

Ms Graham—No, we are more referring to what I was just alluding to earlier, which is legislation or proposals being put out to wide public consultation in the first place.

Senator STOTT DESPOJA—I might just add for the record—and you may well remember this, Ms Graham—that some of us have made attempts to form select committees that deal with

the privacy issue in a holistic manner. But, all of that aside, speaking of legislation or committees, you also talk about the kind of legislative regime or protection regime that we would need if a smart card were to be introduced. You make it very clear that you are not talking about disallowable instruments; you are talking about a legislative regime. Is there anything in particular that you want to bring to the attention of the committee in relation to those legislative protections? Are you talking about stand-alone piece of law or are you talking about incorporating into the currency privacy law the kind of protections and security you think are necessary?

Ms Graham—I do not have specific comments on what would need to be in a law relative to those usages. I would need more detail than is currently available on the actual proposal. But, generally, we are saying that there would need to be specific legislation relative to those specific initiatives. We believe that one problem with the Privacy Act is that it is too high-level. It is too much formed from high-level principles. When you get down to specific uses and purposes, it is too general. I should make clear too, of course, that it would be the information privacy principles that would apply to the Medicare smart card and currently I am more familiar with the national privacy principles, so I will just use those as an example for the moment because they are very similar. But you can interpret certain aspects of the national privacy principles to the left or to the right, so to speak. They can be interpreted to have a privacy protective intent or you can interpret various words and phrases slightly differently and produce a non-privacy-protective intent that favours the business as distinct from individual whose privacy is concerned.

The national privacy principles were only ever intended to be high level principles in the first place. The government—and, presumably, the parliament—anticipated that industries would develop privacy codes that would enhance privacy protection by starting off from the base position of the high level principles and then develop rules and regulations within an industry code dealing with the circumstances in which information could be collected, used, disclosed. But this has not happened. Virtually no industry codes have been developed at all.

It has been said, I understand, in submissions to the Privacy Commissioner's inquiry and so forth that the basic reason that industries have not developed codes is that it is just too expensive and that to have a code they then need to have a complaints process and an adjudicator relative to their own code, so it all becomes exceedingly expensive for industry. Therefore, we have all been left with high level principles that often you can argue till kingdom come as to what this particular privacy principle means in relation to this specific disclosure of information. That is why we believe that, if things like smart cards are going to be used for Medicare with these databases where you can access your personal information, instead of just having high level principles we need actual law that says the only people who can access the back-end database are this organisation or this government department or this set of people, instead of guidelines that just broadly say, 'If it is necessary to have access, then you can have access' and exemptions to the privacy principles that are very broad by saying that law enforcement can access information if it is necessary for the investigation of some law. We do not believe that those kinds of very broad exemptions should apply to people's medical and health information that would be in a Medicare smart card kind of arrangement. We believe that there would need to be a narrow set of exemptions from prohibition of disclosure. There would need to be clear rules about who could and could not access the information, not just these high level principles.

Senator STOTT DESPOJA—Obviously, that is one problem you have identified. The second, which I think makes a difference between whether it is a light or soft touch or a comprehensive regime, is the issue of enforcement and penalties or whatever you think is appropriate. You refer to that in your submission. Can you give examples of where you think there should have been stronger enforcement provisions in the act—whether that is a specific example of a case or an instance, or a general reflection.

Ms Graham—Just a general reflection that it is almost impossible for an individual to enforce their supposed privacy rights. Basically, you have to make a complaint to the Privacy Commissioner, and you wait for the Privacy Commissioner to make a decision. If the Privacy Commissioner chooses to issue a decision under section 52—there is a specific section that refers to a determination—and finds against the business, and then the business does not then comply with the Commissioner's findings, then you can go to the Federal Court and you can ask the Federal Court to, in effect, enforce the commissioner's decision. However, at that point the court does not just enforce the commissioner's decision; the court reviews the whole complaint and makes a decision afresh. So at the moment for an individual to enforce their alleged rights, it is a very complex and expensive exercise. You may be lucky and have the commissioner make a decision quickly and the business just agree to do that—and that certainly does happen with some smaller aspects. But if you have a serious breach of privacy, it is more likely that you will end up having to go to the Federal Court to get the decision heard again. We think that is too hard for most people—too hard and too expensive.

Senator MASON—Again, you are arguing that delineating privacy principles in the Privacy Act is not always the best route to enforcing privacy rights, but that, rather, a prescriptive regime about precisely who and where information could be shared is much better for protecting privacy rights. That is your argument.

Ms Graham—Yes.

Senator MASON—Could we move off that for a second. Senator Stott Despoja again asked a question relating to contemporary issues. A while ago I read in the paper an article by a friend of Senator Bolkus, former Senator John Stone, who fought against the Australian Card back in 1986-87. He has said that he would now consider supporting an Australia Card. His argument was that it would regularise information flows—in a sense along the lines that you have said. So, rather than having tax file numbers here, Medicare cards with chips in them, drivers licences and so forth, an Australia Card could regularise this sort of information and you could prescribe precisely for what purposes it could be used et cetera. Do you think that is an appropriate response? I should say that he also said it would help us fight the war against terror as well. What would you say to that?

Ms Graham—You are suggesting that what he was saying was along the lines of what you thought I was saying, but that is certainly not what I was saying because I am not at all suggesting that we should have any kind of centralised government access to any kind of data. The Medicare smart card is specifically supposed to be for health and medical matters. My understanding is that whatever Mr Hockey is said to have said yesterday has something to do with now connecting that to welfare. I have heard whispers about that over the last couple of years. Certainly EFA would be 100 per cent opposed to having any kind of card where you have medical and health information but then you add welfare to it and then you add something else.

That is then becoming an Australia Card and we are absolutely opposed to that. What I am talking about in terms of having particular laws regulating access is specifically so that you can have the access applicable to medical—

Senator MASON—I understand the point. I do not want you to just go on for 10 minutes. I was merely saying that former Senator Stone now thinks that the Australia Card would be a good idea.

Ms Graham—I am sorry, Senator, but whatever he may think to be the case, that is not what EFA thinks is the appropriate current situation. I do not mind what he thinks. He is entitled to his own opinion.

Senator MASON—As I said, he said that it would regularise the flow of information. He thinks that at the moment the information available—

Ms Graham—I would ask this question: why do we need to regularise the flow of information? EFA would consider that the less flow of personal information there was the better.

Senator MASON—Even if that inhibits the provision of government services?

Ms Graham—I do not see why it necessarily limits the provision of government services. Government services ought to be able to be provided in a way that takes into account the appropriate level of privacy protection relative to the particular government service, and I do not think that there should be a situation where to get any particular government service this is the set of information or rules that applies to this particular service. I believe we have various government departments that deal with various issues and it is perfectly appropriate to have different disclosure and collection regulation relative to what that particular department needs. We should not just say that, because the department of ageing needs this information for that purpose, therefore the tax office can have that information as well. I just do not agree with a set of rules across all government. I think it depends on the specific use and purpose of the provision.

Senator MASON—Would you accept that the government needs information to provide welfare?

Ms Graham—Of course. I do not believe anybody has argued with that. I am not saying government should not have access to information; it is a question of who else they are sharing it with, including within government.

Senator MASON—Sure, but remember that governments have to check whether the information they have been provided with is true because they are giving welfare and there is a welfare budget and they have to be able to check whether the information is true—and you know that.

Ms Graham—Absolutely, and EFA has never argued that they should not be able to do that.

Senator MASON—It is easy to speak for principles as you are but, believe me, when one is looking after the budget, sure, one is concerned about privacy, but there are other competing

issues—and one is honesty. You cannot assume that everybody is honest. I will move on to a question about technology. Some of the submissions say that one of the issues about biometric information is that when the information is taken it is taken forever. Classically it was fingerprints, but today biometric information can be the shape of someone's face, retina identification information and so forth. This may sound like a science fiction question, but are we at the stage now where technology is available such that, with certain biometric information such as the shape of people's faces and so forth, a football crowd could be scanned and people identified and picked out?

Ms Graham—Certainly the proponents of that kind of technology say that that can be done. My understanding is that actual testing of the accuracy of such systems gives rise to serious concerns about accuracy. They will claim that they can pick a particular face out of a crowd, but whether they can actually do that depends on numerous circumstances relative to the quality of the photo, the angle of the person's face and numerous other things. It is argued that that is right on the doorstep of being accurate but it is not at the moment. That is not just the case for the football crowd or whatever; it also applies to the biometric Australian passport photos at the moment. This technology will only work provided you have specific lighting and specific face angles. There is a whole range of issues about exactly how the photo has to be taken for it to be able to be analysed by software after that. It barely works now, when you are just taking a photo of an individual; it is even less accurate across a football crowd. The proponents of the technology will try to claim that it all works perfectly and that we should implement it and be using it all the time because it will help us catch terrorists. It is basically nonsense: it will not.

CHAIR—Thank you for your submission. I thank you and all the other witnesses for some valuable contributions.

Committee adjourned at 12.22 p.m.