



COMMONWEALTH OF AUSTRALIA

Official Committee Hansard

SENATE

SELECT COMMITTEE ON INFORMATION TECHNOLOGIES

Reference: e-Privacy

TUESDAY, 5 SEPTEMBER 2000

CANBERRA

BY AUTHORITY OF THE SENATE

INTERNET

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

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

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

SENATE
SELECT COMMITTEE ON INFORMATION TECHNOLOGIES

Tuesday, 5 September 2000

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

Senators in attendance: Senators Ferris, Harradine and Lundy

Terms of reference for the inquiry:

To inquire into and report on:

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

WITNESSES

CLARKE, Dr Roger, Principal, Xamax Consultancy Pty Ltd.....	168
BURSTON, Mr John, Group Manager, IT Services Group, Department of Employment, Workplace Relations and Small Business	177
FAGET, Mrs Patricia Joyce, Director, Privacy FOI Ombudsman Team, Corporate Legal, Parliamentary and Audit Services Group, Department of Employment, Workplace Relations and Small Business	177
JOHNSON, Ms Marie Helen, Group Manager, Online Services Group, Department of Employment, Workplace Relations and Small Business	177

Committee met at 6.35 p.m.

CHAIR—I call the committee to order and declare open this public hearing of the Senate Select Committee on Information Technologies. On behalf of the committee I welcome all witnesses appearing at this hearing tonight and thank them for their attendance.

Tonight's hearing is the third public hearing of the committee's inquiry into e-privacy. The terms of reference of the inquiry refer the committee particularly to the following issues: the protection of consumer information obtained through electronic transactions; the privacy and disclosure obligations of organisations that have access to consumer databases; and the access by consumers to personal information held in consumer databases.

Before we begin the hearing I note that the committee has received three pieces of additional information provided in response to questions placed on notice at our previous hearings. They are from the Electronic Frontiers Association, EFA; the Australian Internet Industry Association, AIIA; and the Australian Retail Group, ARG. Is it the wish of the committee to receive this additional information and authorise its publication?

Resolved (on motion by **Senator Harradine**):

That the committee receives the additional information and authorises its publication.

CHAIR—All witnesses should be aware that the committee prefers evidence to be given in public. However, witnesses may at any time request that their evidence or any part of their evidence be given in private and the committee will consider any such request. I point out, however, that evidence taken in camera may subsequently be made public by an order of the Senate. I also remind witnesses that the giving of false or misleading evidence may constitute a contempt of the parliament.

[6.36 p.m.]

CLARKE, Dr Roger, Principal, Xamax Consultancy Pty Ltd

CHAIR—Welcome. The committee has before it your letter marked as submission No. 21, which refers us to your published work. We also have before us a supplementary submission numbered 21B. Is it the wish of the committee to receive the supplementary submission and to authorise its publication?

Resolved (on motion by **Senator Lundy**):

That the committee receives supplementary submission No.21B and authorises its publication.

CHAIR—Are there any alterations or additions that you would like to make to your submission?

Dr Clarke—No, thank you, Senator.

CHAIR—I now invite you to make an opening statement and at the conclusion of your remarks we shall proceed to questions.

Dr Clarke—Thank you very much and thank you for the opportunity to provide a supplementary submission. First, a very brief background, which is necessary to establish the framework from which I am coming. I am a consultant in electronic business and have been since long before the term was invented; also, in information infrastructure and in dataveillance and privacy. I spent a decade as a senior academic in information systems and I have undertaken research, consultancy and advocacy in the area of privacy generally for nearly 30 years.

I have undertaken research, consultancy and advocacy in relation to e-privacy matters since the early 1990s. The first submission that I provided to you, the annotated bibliography, shows in excess of 40 publications which I have put out in the specific area of e-privacy. That means a number of things, both positive and negative. One of them is that I have very broad coverage across the entire area that I believe your committee is interested in. It also means that I am trying to keep up with enormous numbers of developments in an enormous number of different areas and I cannot guarantee to be fully up to date on every one of them at any given time.

As regards my submission, I have sought to address your terms of reference. Speaking very briefly to the words in the written form, my first concern was that the terms of reference as written contain a couple of potential constraints which I was a little uncomfortable about and I felt needed to be drawn to your attention. I am not suggesting for a moment these are intentional constraints, but they are constraints that are easily read into the wording. The first one is that they are very easily read as only applying to the economic dimension of people's lives. The fact of the matter is that the vast majority of activity on the Internet continues to be other than economically motivated—socially, one-to-one communications, and so forth. Therefore, if that were to be read narrowly this would be a constrained study of e-privacy.

A second concern is that many of the phrasings, particularly in terms (a) and (b), appear to presume—whether they do or not—that marketers have some kind of innate right to gather, to use and, in particular, to interchange personal data. That is something that may be mainstream thinking in some parts of the United States, mainly business, and it may be accepted by the current Clinton administration in the United States. It is certainly not mainstream thinking anywhere else in the world, and it may well not be mainstream thinking in the incoming administration next year, particularly in the event that Vice-President Gore were to take the presidency.

I have submitted that, in the United States rather than in Australia, e-privacy issues are going to force a change in the stance of the United States, to the extent that legislation for privacy more generally will become quite inevitable in the US as a result of e-privacy concerns. I am finding, since I published that 18 months to two years ago in a leading US journal, that I am getting more and more echoes of that argument coming back to me from many different sources. I believe it is not appropriate to accept any forms of presumptions that marketers have any special standing.

The third aspect I wanted to briefly highlight was that the Internet is a broad piece of infrastructure which is used for many different purposes and, indeed, used in many different ways. To put it a different way, it is a cluster of technologies, or there are many subtechnologies running over it. The term that is used in one of the terms of reference here is the word ‘browsing’, and the word browsing is most commonly only used in respect of one of those services. Admittedly the World Wide Web dominates our thinking in so many respects and is the primary means whereby we all pull information down from the Net when we go looking for it, but it is only one of the order of a dozen services. It would be unfortunate if you were to accidentally restrict your terms to only look at the World Wide Web component of the Internet. Those are the qualifications in relation to the terms of reference.

I have a couple of quick points about privacy law. It is commonly assumed that the OECD guidelines are the standard to which laws aspire. I need to draw attention to the fact that the OECD guidelines were codified around 1980, but what they codified were laws that had been passed in the period 1970-75, and those laws had been addressed at information technology of the late 1960s. To the extent that a new piece of legislation right now fulfilled the needs or aspirations of the OECD guidelines, we would be 30 years, or a little more, behind. The OECD guidelines, which implement so-called ‘fair information practices’, as it is usually called, are a completely inadequate approach at the turn of the 21st century. Nonetheless, we are still behind, specifically in the private sector, and in most public sectors in the Australian states and territories, and we badly need to catch up to 1970 to start with.

I would now like to address the terms of reference one by one. In relation to term of reference (a)(i)—and I have divided your term of reference (a) in two because I believe it has a natural split—where the Internet is concerned, it is extremely important to appreciate the nature of Internet technology and Internet architecture, and to appreciate the nature of the various technologies that run over it. These are very different from technologies that have gone before, and the attempts to argue by analogy—be it from highways, be it from railway lines, be it from broadcast media like radio and television—have all been singularly unsuccessful. The Internet is itself, and needs to be studied and understood in its own terms.

There have been some very disappointing attempts by a variety of organisations, including this parliament, to deal with various aspects of the Internet during the last five years. Some of the severe disappointments that many of us—as consultants, researchers, academics and advocates—have felt have been measures by organisations like the GPKA, the Government Public Key Authority, in relation to digital signatures, and also the National Electronic Authentication Council, NEAC, which have dramatically failed to understand the nature of the technologies and their privacy implications. We have also seen seriously disappointing actions by people like the Privacy Commissioner, whose guidelines on workplace email, web browsing and privacy, again, fails to get to grips with the needs of the public in those contexts. I believe that, as a conclusion from that, a great deal more effort is needed to come to grips with the technologies and their implications, and that is by all and sundry.

In relation to terms of reference (b) and (c), consumer marketing databases, there is a very serious concern amongst many of us in the community, and amongst those of us who consult to such marketers, that marketing organisations have failed to understand Internet technologies, that they have failed to understand cyberspace behaviour and that they have failed to understand that e-consumers are a completely different breed from conventional consumers. They have continued to exhibit exploitative behaviour which works for them when they have broadcast media to deal with or to use to reach consumers. The Australian Direct Marketing Association is the most obvious of the organisations which has completely failed to understand and deal with those changes. Its code is objectionable enough in relation to mail and telephone marketing, but it completely misses the point in relation to marketing over the Internet.

I have a couple of final points to make about policy aspects. Firstly, there is a bill before the Senate which has been claimed by its proponents to provide protections to the public in the context of private sector behaviour. It simply does not. It is an appalling bill which falls so far short of any expectations—at the levels of the OECD guidelines—as to be a complete con on the Australian public. I have documented at length—and will be documenting again on this matter before the other Senate committee—the litany, in the order of 50, of major deficiencies which make it not a privacy protective bill but a sham. It is a bill that sets out to legitimise privacy invasive behaviours by the private sector and it badly needs to be rejected. If it is not rejected by the Senate, if it is passed into law in any form, it will seriously undermine the relationship between consumers and corporations.

Secondly, we have a serious need to move beyond the OECD guidelines, which, as I pointed out, we have not even reached yet. However, we have to be very careful in how we do it because we need the framework in place of an OECD style statute and we also need to consider some of the broad policy differences between the Internet environment and what has preceded it. One of those issues, for example, is the suprajurisdictional aspects of the Internet—that is, the extent to which it is more difficult than it used to be to reach people and control their behaviour. It is not impossible. Geographically based jurisdictions have difficulties because people who wish to can contrive to have their behaviour appear to be in several places at once or scattered across several jurisdictions. Therefore, it is very hard for any one jurisdiction to prosecute. However, it is not impossible to prosecute—it is merely more difficult—and each jurisdiction has a responsibility to set rules of fair play for its own society.

However, to move too quickly would be to make some serious mistakes. Because the Internet is so different and so recent and so hard to come to grips with, it is very easy to come forward

with poorly-shaped laws. There are a great many of them that have been brought before this parliament and proposed by various parts of the Public Service. One of the vogue ideas around the Public Service is the notion of technology neutrality. It is not only in vogue in the Public Service but it has also been happily accepted by quite a range of other organisations. I submit to your committee, however, that the concept is dubious in any context and, in the Internet context, it is a vain hope. The point about technology neutrality is this: each technology that comes does not simply replace, one-to-one, the predecessor technology. It inevitably comes from a different direction entirely. It is more encompassing—it comes with different objectives in mind, with different capabilities and with different opportunities embedded in it. Attempts to frame legislation which we believe will regulate technologies that have not yet been dreamt of are simply a vain hope in a context like the Internet. What we have to do is to appreciate that yes, some principles and some aspirations for outcomes are common and only change very slowly, but the detailed forms of regulation which many technologies and many behaviours of the private sector and of government require need to have quite specific and quite targeted legislation.

As I have suggested, these measures are still new and we are still learning to cope with them. I would be very concerned if the parliament were to move too quickly to regulate the Internet. My strong belief is that the role parliament should be pursuing right now is investigating these issues—as your committee is doing—and creating mechanisms to ensure the ongoing study of rapidly changing phenomena. Wouldn't it be nice if there were an office of technology assessment to which your committee could refer a range of questions which require deeper study? Finally, your committee could deliver early warning signals to business about the importance of privacy and the inevitability of early legislation. Thank you.

CHAIR—Thank you, Dr Clarke. I draw your attention to the comment you make on page 2 of your submission where you say:

Many corporations marketing to Australian consumers have been extremely cavalier in the handling of personal data.

Could you elaborate on ways in which you are aware corporations have been cavalier? I am not expecting you to name any, but we are trying to canvass some marketing operations existing within the code of practice that you—and others—have found to be cavalier.

Dr Clarke—Yes. There is a number of different elements to this, and that is the reason for my pausing and giving myself a couple of notes to work from. The first couple precede the Internet but have become sharpened by the Internet. The first is lists of various kinds: mailing lists. There has been a presumption by the private sector that the kinds of behaviours that a person exhibits in terms of attendances at conferences and home shows in exhibition centres, subscriptions to magazines and so forth are fair game for any organisation in the private sector to latch hold of and to combine in order to build profiles of individuals.

Another presumption that has been made by many corporations is that information on so-called public registers—a concept which, by the way, I have argued strongly against; I think it is a nonsense concept but it does exist in the Privacy Act 1988 regulating the public sector—is available to them to be used for whatever purposes they believe are appropriate. They have even made further presumptions that documents like the *White Pages* run by telcos are public registers and should be raided and used. Each of those presumptions is not accepted by consumers and needs to be challenged and rolled back and behaviours need to be regulated.

More recently in the Internet context, we have seen a range of techniques developed, and in some cases techniques subverted, to enable the gathering and inferring of information about net consumers from their behaviour on the Internet. These tend to be hit and miss, probabilistic rather than certain ways of collecting data, but when you are dealing with large quantities—which is what many of these marketers are doing—you can gather a great deal of data off the Internet. You can be 70 per cent or 80 per cent right and develop further data that enables you to profile consumers and thereby manipulate their behaviour through selective presentation of advertising.

CHAIR—On page 7, you refer to what you call a particularly extreme initiative: the Acxiom InfoBase, which came to light in November 1999. Would you like to tell us why that is an extreme initiative?

Dr Clarke—From what we have been able to establish about the Acxiom initiative, it appears that basically every technique I have mentioned in the last few minutes, and more besides, and every source that we have been able to document over the years is being gathered together by one particularly large pair of organisations—one Australian, one foreign—to consolidate consumer profiles and to store them in one of the more permissive states in the United States, which is, of course, a country that is quite limited in terms of privacy protections. It is every one of the nightmares that consumers have being lumped together in one initiative.

CHAIR—You are saying that when somebody buys a magazine subscription they could find themselves on a database without even knowing it. Are you perhaps suggesting that, in trying to look at ways in which this committee might address some of the issues that you and other witnesses have raised, there would be some capacity for an opt-out provision on subscription forms, hotel registers, your telephone account or on some of the other quite innocuous-looking documents that might come to your house or innocuous-seeming actions that an individual might take that find their way to a database? Would that option appeal to you?

Dr Clarke—Only very little. There are three alternative approaches. There is *carte blanche* which the industry believes it has right now; there is opt out—that is to say, you are in unless you specifically signify that you are out—and the other alternative, the privacy protective stance, is opt in which is permission based marketing where informed consent is required from a consumer before data is used. The stance that most people would adopt, I believe, is that society exists for the purposes of the individuals in it. Corporations are a fiction of the nineteenth century which have proven to be extremely convenient for us, but they have not become the purpose of our society. They are still servants of society, and corporations should be required to comply with social needs. Therefore, opt in should be the norm, and where that probably considerable number of consumers, choose to opt in and to tick the box to have their data shared or reused for particular purposes, then that is the appropriate approach to take. What is more, in one of my papers on direct marketing and privacy, I have shown the number of different ways in which effective marketing can be achieved using opt in techniques. It is not, despite ADMA's protestations, the death of consumer marketing if you close out and if you move beyond opt out to opt in.

CHAIR—A number of other questions spring to my mind but I will go to my colleagues, Senator Lundy and Senator Harradine, and see how we are going for time.

Senator LUNDY—Referring to page 4 in your submission, you identify a number of privacy invasive technologies—PITs—noting cookies, spam and single pixel image tracing methods. But I particularly wanted to ask you about the public infrastructure to support digital signatures. Could you extrapolate on your specific concerns and why, in your view, that technology is a privacy invasive technology?

Dr Clarke—The notion of digital signatures is very attractive because it enables people using private keys that only they possess to indicate that they are the originators of messages. The problem is the way in which cryptography has been applied in order to produce that capability: it has been produced by engineers who have not considered their public policy implications. The first mistake that they made with contemporary technologies is that the sole way in which you can affix a digital signature is by identifying yourself. In other words, every digital signature and every certificate saying that it is your digital signature is assigned to a unique identity. There are many circumstances in which a unique identity is not appropriate.

There are many circumstances in this society where people either use anonymity or they use pseudonymity—that is, multiple alternative names in different circumstances. The way in which PKI has emerged denies that. It also creates the risk that the public key—the other half of the key that is used by the reader of a message to check that the message was, indeed, signed by the person it purports to come from—could easily become a de facto unique identifier for individuals. That would, of course, be very much against the interests of the Australian public, as they indicated in 1987 with their reaction to the Australia card proposal when they understood what it really meant. My belief is that the Australian public still feels the same way about unique identifiers. The idea of a single private key public key pair is anathema to the Australian public.

Similarly, even if there were a single key you could have multiple certificates so that at least multiple certificates would declare that it was your key and you could use alternative certificates in different circumstances. But unfortunately they would be too easily correlated. You would end up with perhaps several identities associated with your certificates but they would be so obviously associated with the same key that those certificates could become a de facto national identifier as well. Essentially, the problem is that, while it would be possible to come up with a public key infrastructure that would be privacy protective rather than privacy abusive, the existing technology does not support privacy friendly digital signatures.

Senator LUNDY—Going a little further on that, is there any technology to support digital signatures that, in your belief, constitutes a privacy enhancing technology?

Dr Clarke—There are some fairly well developed standards and techniques around—the popular words are either PGP, for pretty good privacy or SDSI, and I cannot for the life of me remember what SDSI stands for, we are so used to four-letter acronyms in the IT industry—which adopt a quite different approach to public key infrastructure and which involve, rather than one organisation certifying, multiple friends in a ring, in effect, certifying. That provides a much more democratic approach rather than the hierarchical approach that conventional public key infrastructure adopts.

Conventional public key infrastructure is effective and will be installed in places like the Australian Defence Forces, because that is an organisation that is, and needs to be, arranged

fairly hierarchically—there are delegations of command and control. It does not work in society because society is much more pluralistic than that. So, yes, there are alternatives. To be fair to the people who are trying to implement PKI, these other technologies are not quite as far advanced as the wrong kind of PKI.

Senator LUNDY—In terms of the need for digital signatures to verify identity in the current electronic environment, do you have a view on how that problem of having an individual electronic identity can be resolved in the short term without public key infrastructure?

Dr Clarke—There are many presumptions made by many people, even Internet specialists, that digital signatures are about authenticating identities. That is quite wrong. I have published a succession of papers which have shown that authentication is a quite general concept. Authentication is about developing confidence in some kind of assertion. An example of an assertion that has nothing to do with identity is an assertion that this particular thing or this particular string of bits has got value. We used to hold notes up to the light and check for the metal strip; these days we look for the hologram on the note. That is a form of value authentication, and we can do the same kinds of things on the Internet without ever knowing about identity.

The reason that is important is that the vast majority of transactions that individuals have conducted historically have been anonymous. They have been marketplace transactions, they have been cash based transactions, they have been pouring oneself a cup of coffee, having a conversation in a bus—unknown identities. The way in which people are trying to develop the Internet is taking away from the public the scope to be anonymous like that. So the first thing we need to do is appreciate that authentication techniques can be of value, or even of eligibility or credential. That is to say: is it critical that you know that this person is Dr Bloggs or is it critical to know that this person is a doctor who is authorised to do certain things, such as perform certain treatments or to make certain claims under the health insurance scheme? Really, it is the eligibility or credential that is critical.

There is actually a very small number of circumstances in which identity is crucial to society's workings. Every time I publish this overhead slide that I use of the list of things that I cannot solve without identity, somebody in the audience shows me a reference in the literature that shows another one is wrong and it can actually be done. An example is credit cards. Most of us would assume that you cannot do credit card transactions anonymously. In fact, that was one of the first that was knocked down at AT&T's research labs in Florham Park, New Jersey: when I presented there 18 months ago, they showed that they have a prototype running in their laboratory which explicitly runs effective credit card schemes anonymously. So what we have to do is appreciate that we must not leap to the first and obvious thing, which is hierarchical solutions and identity everywhere. Let us work out what our real requirements are and build technologies on the Internet that will service the real social needs.

Senator LUNDY—Thank you. I have another question in relation to your comments about the inadequacy of the philosophical underpinnings of the OECD guidelines and your point about technology neutrality perhaps not being a relevant starting point in considering laws with respect to that particular example on establishing identity and also to how people manage their personal identity, including privacy issues. I am conscious of time, Chair. I do not know,

Dr Clarke, if you have any additional points you want to make on that, but it is certainly of interest to me, given this tendency for us to assume that somehow technology neutrality is desirable in the first instance.

Dr Clarke—It is very attractive but, unfortunately, it is also very difficult. Let me give one example that may be straightforward enough—most of them are quite complex ones. It has been presumed by marketers and ADMA, at least, that email should just proceed on the same basis: unsolicited emails can be sent to people and, under technology-neutral law, opt out mechanisms will be sufficient. It turns out that the existing models of physical mail, ‘snail mail’ letters through the post, and telephone marketing, ‘outbound telemarketing’, as the marketers call it, are based on one set of assumptions about technology and one set of assumptions about economics. That assumption is that the caller, or the initiator, pays. The receiver does not pay money; the receiver might well pay, in terms of time and interruption, but they do not pay money.

With email, it is, in fact, the other way round. Because of the nature of the technology, it is the recipient of the email who has to download the thing, and particularly when it is large—and they are getting larger as HTML starts creeping into our email and as people start loading up attachments with nice little video clips and sound clips—as these things happen, our mail boxes are getting larger and larger and our download times, especially if you are unfortunate enough to live outside a capital city and you have slow download times, are slower and slower. I travel on the road a lot, and when I download from various places around the world at 22 Kbits per second, I am finding megabyte attachments to some of these things. It is extremely hard to handle that in a hotel room overseas, so I feel for some of my fellows in the country.

In other words, the inconvenience is at the recipient’s end and it is very substantial, and so is the money. The actual payments are made by the receiver. Any presumption of technology neutrality working there is wrong, and ADMA’s blithe presumptions that things they have got away with in telephone marketing should, therefore, be fair game in Internet marketing are completely unjustified.

Senator LUNDY—Thank you.

Senator HARRADINE—Very briefly, what is wrong with the coregulatory approach?

Dr Clarke—I have, in fact, been a champion of ‘coregulatory’ in its original sense of the word. Coregulatory sits between the extremes of black letter law and everything enshrined in legislation and the nonsense of pure self-regulation at the other end. Coregulatory has the advantages that there is, or should be if it is implemented properly, a framework established by the parliament, but within that framework the details of individual sectors and the details of individual business practices can be taken account of and a detailed code can be established in such areas as marketing, health and so forth. In fact, if coregulatory is implemented properly, then I am a strong fan of it and I have a number of papers which express and explain what it is.

Senator HARRADINE—Yes, but you are not confident of some of the codes around the place at the present moment?

Dr Clarke—Highly lacking in confidence in the codes, because, at the moment, we do not have a coregulatory proposal. We have a strange mixture of too much in the statute with too many exemptions and, at the other extremity, we have codes being developed by quite a few of the industry associations which are quite inadequate and do not measure up to anything like OECD standards.

Senator HARRADINE—You mentioned OECD standards and you expressed some doubt about them as they are based, according to you, on 30-year-old technology. Isn't it important to have such guidelines, even if only for the fact that persons wishing to conduct e-commerce with the European countries that are going along with the OECD cannot do so unless they are committed to those?

Dr Clarke—Yes, the EU directive, I believe, is for economic reasons important to Australia. I think it would be highly beneficial for Australian organisations if they were subject to an OECD equivalent law. In fact, it is slightly more than the OECD, because the EU directive already brings it slightly further. Yes, I am a strong supporter of an OECD style legislation, not the bill that is currently in front of the Senate.

CHAIR—Dr Clarke, I understand that you have very generously offered some extra time to the secretariat staff to work through some of these issues as we put our report together. I would like to express the committee's gratitude for you offering to do that. I know that the secretariat staff will find that very helpful. I apologise that we have to move on tonight, but perhaps we can leave it that if the committee could get back to you in due course as we work through the issues we would be very grateful. Thank you very much for making yourself available this evening.

[7.10 p.m.]

BURSTON, Mr John, Group Manager, IT Services Group, Department of Employment, Workplace Relations and Small Business

FAGET, Mrs Patricia Joyce, Director, Privacy FOI Ombudsman Team, Corporate Legal, Parliamentary and Audit Services Group, Department of Employment, Workplace Relations and Small Business

JOHNSON, Ms Marie Helen, Group Manager, Online Services Group, Department of Employment, Workplace Relations and Small Business

CHAIR—The committee has before it submission No.29, which it has already published. Do you wish to make any alterations to that submission?

Mr Burston—No, Senator.

CHAIR—I now invite you to make an opening statement and at the conclusion of your remarks we will proceed to questions.

Mr Burston—Senator, we do not have any opening statement to add to what we have in the submission.

CHAIR—Thank you. Perhaps we will go to Senator Lundy.

Senator LUNDY—Thank you. In reading your submission I have got questions for all areas but I think I should focus on the Business Entry Point web site and issues particularly relating to recent events and challenges with respect to the privacy management of that site. I was hoping you would be able to, in the first instance, provide an update about the activities of DEWRSB in addressing privacy issues in particular in relation to the Australian Business Register online on the Business Entry Point site.

Ms Johnson—I will answer that question with an update and perhaps a point of clarification on the Business Entry Point and the Australian Business Number online registration. Subject to the legislative changes which occurred back in June—I am not sure of the exact date—the 16 fields in the full ABR are now not available to anyone but the owner of that record. Previously the full record of the ABR—and there are 16 fields—was able to be accessed for a fee of \$20, which was stated in the legislation. That access to the full ABR record was not able to be undertaken online. What was available online and what is still available online is a subset of the ABR containing 10 fields, which is available for look-up online. That has always been the case—it was the case prior to the legislative change.

In addition to the legislative changes that occurred, in consultation with both the ATO and the Privacy Commissioner, our privacy statement on the BEP in relation to the ABR was made more prominent, so that the privacy statement was drawn to the attention in a more obvious way than it perhaps had been, although the privacy statement was in existence in its form prior to the changes that were made. That is in essence the update. I will probably get more questions.

Senator LUNDY—I am appreciative of that. You mentioned legislative change that managed the shift from what used to be available for \$20, albeit not online, to now not being available. At what point was that legislative mechanism introduced and dealt with, and what was the legislative mechanism? Or was it a regulatory mechanism or a ministerial—

Ms Johnson—No, the legislation was changed.

Mr Burston—Would you like us to get the detail and come back to you on that, Senator?

Senator LUNDY—Yes.

Mr Burston—We will take that on notice.

Ms Johnson—The legislation was changed. I can get back to you on the details and the date it was changed.

Senator LUNDY—In terms of actual dealings through parliament, there has been no process of passage of amendment bills in relation to that so—

Mr Burston—We will come back to you on the detail.

Senator LUNDY—I am just presuming it was a ministerial regulatory mechanism.

Ms Johnson—We will provide you with the details, but it is my understanding that the legislation itself was amended.

Senator LUNDY—Okay. Could you also come back to us with full details about that process?

Ms Johnson—The process by which the legislation was amended?

Senator LUNDY—Yes, that would be great. The other issue raised at the time was the distribution of a CD-ROM which effectively had the database of ABR information on it. Could you provide me with an update on how the distribution of that database is now managed, both before and after the changes?

Ms Johnson—A point of clarification. When we last appeared that issue was raised. The issue was, in fact, that the database was not distributed on CD or via any other medium. What was undertaken was that there was a subset of the ABR database containing 10,000 entries and a subset—

Senator LUNDY—How many fields in that?

Ms Johnson—It is my understanding that there are five fields. The full ABR has 16 fields. There were five fields, 10,000 records, which were made available to a number of information brokers for the purposes of testing their systems for getting ready for GST so that their subscribers, their clients, would be GST enabled. That was for the purpose of a test to see

whether that was a reasonable and technically feasible thing to do. Since that time, there have been three arrangements entered into with three separate information brokers in which copies of those five fields that I have spoken about have been provided to the three information brokers for the purposes of amending their systems and appending the ABN to their systems.

Senator LUNDY—Of the full database?

Ms Johnson—No, the five fields. Five fields were chosen.

Senator LUNDY—Yes, five fields, but all of the records?

Ms Johnson—Yes.

Senator LUNDY—How many records are there altogether?

Ms Johnson—On the ABR?

Senator LUNDY—Yes.

Ms Johnson—I will have to take that on notice, but I think it is in excess of two million.

Senator LUNDY—Okay. Who are the three information brokers?

Ms Johnson—Dun and Bradstreet Australia Pty Ltd, Australian Business Research Pty Ltd and Credit Advantage Ltd.

Senator LUNDY—What is the business of those organisations? I am familiar with Dun and Bradstreet. Perhaps for the record you would like to describe what each of those organisations does. Is Credit Advantage a statutory authority?

Ms Johnson—No, it is not. I will have to take it on notice to give you more details about the nature of their business. Apart from saying—sorry?

CHAIR—I was just pointing out to Senator Lundy they did give evidence in Sydney.

Senator LUNDY—Yes, I thought I recognised the name.

Ms Johnson—So, just as a point of clarification, do you require us to come back to you with details of the business?

Senator LUNDY—Yes, just those three, and also the date on which that information was distributed, particularly in relation to the changes that took place.

Ms Johnson—Okay. I have got some of that detail here, but I can give it to you in full.

Senator LUNDY—Please—if you have got it there.

Ms Johnson—The date that the agreement with Dun and Bradstreet was entered into was 29 June 2000; in relation to the Australian Business Research Proprietary Ltd, the date was 29 June 2000; and with Credit Advantage Ltd, it was 10 July 2000.

Senator LUNDY—Did you charge anything?

Ms Johnson—There is a service fee associated with the provision of that data.

Senator LUNDY—What is that?

Ms Johnson—The dollars?

Senator LUNDY—Sorry, yes, the actual cost.

Ms Johnson—The service fee for the initial provision of the data is \$5,000 and there is a \$1,000 update charge on each occasion that we provide an update. That fee is worked out on a cost recovery basis. There is some significant effort in undertaking to provide that detail to the three companies provided, or each of the individual companies provided. That detail includes technical aspects of programming to do the download as well as some significant effort in constructing licence agreements, which actually limit the use of the data that is provided to those information brokers. So there are legislative arrangements that are worked out as well.

Senator LUNDY—Are there legislative arrangements for it?

Ms Johnson—I am sorry, there are legal arrangements, not legislative arrangements.

Senator LUNDY—Are they contained in some sort of licensing agreement?

Ms Johnson—A licensing agreement has been prepared in consultation with both the ATO and the Privacy Commissioner, so that takes into account the restrictions on the use of the data that those organisations are accepting. It also covers the manner in which the companies need to undertake to make themselves available, for example, for audit reports and so on, so there is quite a stringent licence agreement that they sign with us.

Senator LUNDY—How is that distributed? That is actually the circumstance that I had in mind when I said distributed on CD ROM. How do you actually distribute those databases of two million or more records?

Ms Johnson—I will have to get back to you on that on notice. I do believe it is on CD, but I will have to get back to you on notice on that.

Senator LUNDY—How do you qualify to be eligible to receive this database? Obviously, paying the money is part of it, but with these licensing commissions, is there some sort of pre-qualification people must demonstrate to get hold of it?

Ms Johnson—The qualifications are not so much outlined in the licence agreement, but certainly the usage of it is outlined in the licence agreement. The benefit of providing these

companies with this data is that it more enables the implementation of the new tax system by enabling these companies to append the ABN to their customers' details. It means that those customers are then also able to utilise the ABN in their business operations. So, from that point of view, it is not for any purposes other than assisting the implementation of the new tax system.

Senator LUNDY—And that is a condition of you providing the information?

Ms Johnson—I am not quite sure whether it is a condition of providing it, but certainly that is one of the issues that we investigate—that these companies have a clientele that require, as part of their business operations, the ABN. So, appending the ABN to their data systems means that their clientele are able to implement and able to be GST ready.

Senator LUNDY—In terms of the Privacy Commissioner's involvement in negotiating the terms of the licence agreement, the first question is: can you make those terms of the licence agreement available to the committee?

Ms Johnson—Yes, we can.

Senator LUNDY—Secondly, what role did the Privacy Commissioner play in advising you of those terms of reference of the licensing agreement?

Ms Johnson—I can provide you with those details on notice. Certainly, the Privacy Commissioner was engaged with us from the beginning of the drafting of these licensing agreements. If you want more detail, I can provide you with that on notice.

Senator LUNDY—In the context of your response, I am interested in Australian Business Research and how the application of that criteria facilitating the introduction of the GST relates back to that particular client.

Ms Johnson—I will have to get back to you on that one—

Senator LUNDY—Yes, that is fine.

Ms Johnson—Given that I cannot say at this point in time, off the top of my head, what the nature of their business is. Certainly, they would have a client base to which the inclusion of the ABN is beneficial for their clients in the implementation of the GST. I will get back to you in relation to that particular company.

Senator LUNDY—Can you provide the committee with information as to what the 16 fields are in the full business register, what the 10 fields are in the subset that is available for look-up online and what the five fields are that are distributed? Are there any circumstances where you sell, for cost neutral or for whatever purposes, more than five fields of information?

Ms Johnson—No, there is not. I can provide you with the details of what those fields are. To make more sense, I can provide you with a chart that lays out all the fields.

Senator LUNDY—You do not have to do it tonight but that would be useful. I am presuming that the five fields include the name?

Ms Johnson—I can tell you what the five fields are. To go through 16 is probably a little tiresome. The five fields for the ABR bulk provision is the ABN, the status of the ABN, the legal name, the effective date of GST registration and the ACN or ARBN. They are the five fields that we provide in our bulk provision of data to the three information brokers.

Senator LUNDY—Can people buy the subset of 10 fields for \$20?

Ms Johnson—No, there is no—

Senator LUNDY—Individual purchase?

Ms Johnson—ABR Online, which is the online look-up—

Senator LUNDY—They just access that?

Ms Johnson—is publicly available free of charge.

Senator LUNDY—Do you distribute that in bulk in any way, shape or form?

Ms Johnson—No. The five fields that I have just mentioned are the only fields that we distribute in bulk.

CHAIR—I think these might have to wait for estimates.

Senator LUNDY—That is all I needed to know.

Senator HARRADINE—Moving on to the AJS, if you don't mind—the quite impressive figure of 400,000 job searches via the touchscreen and 150,000 via the Internet. That is quite impressive. I am wanting to see how privacy works. You have provided us with attachment B, which indicates the AJS privacy statement. I imagine how it works is that you have a resume and that that is built up. Then that is matched with the applications or the job vacancies notified by employers without name identification and so on. Presumably, the name identification is entirely at the request of the applicant.

Mr Burston—It is at the discretion of the job seeker who lodges the resume.

Senator HARRADINE—Attachment B seems to be directed largely at the job seeker. What about the employer? What privacy conditions apply to the employer?

Mr Burston—In a sense, Senator, they are equal. The AJS system is predominantly about advertising jobs. The tradition is that unless the employer so chooses, the identity of the employer is not displayed on the system. That really harks back to the time of the CES. The CES in those days performed—as, indeed, the Job Network now performs—a very valuable filtering function. If a firm were to put their name with a vacancy they could get 100 phone

calls, of which 80 may be unsuitable. So, on both sides of the ledger, a job seeker in the case of lodging a resume and the employer in lodging vacancies have their identities protected. But, in each case, if they so choose, they can put their identity on the system.

Senator HARRADINE—In Sydney we had evidence relating to CrimeNet. You are aware of that?

Mr Burston—I have heard of the concept but I am not familiar with the details.

Senator HARRADINE—Do you have employers seeking information on that matter?

Mr Burston—Not through our system, that I am aware of. There may be informal dealings through Job Network members and so on, but there is certainly no linkage in any of the IT that we provide to the Job Network or to the touch screen network that attempts to do any of that sort of matching.

Mrs Faget—If I could supplement that by saying that under the terms of our contract Job Network providers are required to adhere to the Privacy Act as if they were covered by the provisions of the Privacy Act so they can only collect information which is relevant and necessary for their function as a broker. They are discouraged from collecting information about criminal history in relation to job seekers. It is up to the job seekers to disclose that. The providers are not able under the employment services contract to do police checks on prospective job seekers.

CHAIR—Because of time constraints I will not pursue a couple of questions. I may put them on notice at a later time. Mr Burston, Ms Johnson and Mrs Faget, thank you very much for making ourselves available to this committee on a weekday evening. We appreciate it and thank you very much for coming.

Proceedings suspended from 7.32 p.m. to 7.44 p.m.

CHAIR—We cannot get through to our final witness this evening, Mr Richard McDonald, representing RNR International Marketing Group, the list and database management division, International List Brokers. Senator Lundy, are you prepared to move that we submit some questions in writing to Mr McDonald?

Senator LUNDY—I think that is the appropriate course of action at this time. I understand he has been very cooperative, so I look forward to his responses. I so move.

CHAIR—Thank you very much. We will make contact with Mr McDonald in that way and consider his answers in due course. Thank you.

Committee adjourned at 7.45 p.m.