PRIVACY LAW ISSUES — REFORM PROPOSALS AND THEIR IMPACT ON THE FINANCIAL INDUSTRY

THE HONOURABLE DARYL WILLIAMS AM QC MP

Attorney-General and Minister for Justice, Canberra

Mr Chairman, distinguished guests, ladies and gentlemen. I would like to thank the Banking Law Association for inviting me to speak at this 14th annual conference which draws together experts in banking law. I would like to talk today about recent developments in privacy.

On 21 March 1997, the Prime Minister announced that the Commonwealth would not be implementing privacy legislation for the private sector.

In making this decision, the Prime Minister made clear that the Government was concerned not to increase compliance costs for Australian businesses, both large and small.

Complying with current regulatory requirements already imposes a significant burden on Australian businesses.

I note that the Small Business Summit in June last year recognised the cost and frustration from unnecessary or overly complex regulation which falls on small business. A specially commissioned survey, *Working Overtime* has found that, on average, small businesses spend four hours a week on "compliance matters". Over the course of a year this costs the average small business $7,000. This Government does not want to add to that weight.

We are committed to reducing the regulatory burden on all business – the introduction of a new compulsory regime would be counterproductive to meeting that commitment.

The Government's decision not to legislate on private sector privacy followed extensive consultation based on a discussion paper released in September last year. That discussion paper outlined a possible approach to privacy protection in the private sector. Its purpose was to enable business and the community generally to provide concrete comments. I also made clear that, through receiving these comments, we aimed to identify the right balance between ensuring adequate privacy protection and advancing the competitive interests of Australian business.

More than 100 submissions were received in response to the discussion paper, many of which provided detailed comments. A number of major banks and other financial bodies contributed their views. As well as formal submissions, a number of organisations took the opportunity to meet with my advisers and the relevant officers of my Department to discuss areas of specific concern.

While overall the submissions rated privacy protection for personal information important, views differed on how this ought to be achieved in the private sector. Some submissions argued strongly that there was no clear need for legislation in order to ensure privacy protection. There was particular concern about how a legislative regime would impact upon small and medium

enterprises. It was considered that concerns could be adequately addressed by business on a voluntary basis.

These submissions reinforced the view of this Government that business knows best how to respond to the needs of consumers. Government intervention in the form of legislation should only be imposed if no other realistic alternative is available.

In announcing the Government decision, the Prime Minister announced an alternative approach to ensuring privacy protection in the private sector. The Prime Minister announced that the services of the Federal Privacy Commissioner would be made available to assist business in the development of voluntary codes of conduct and to meet privacy standards.

There is a strong case for business to pursue a voluntary approach to privacy. Most people – and that means business customers – dislike uninvited intrusions into their private lives. They like to have some control over information that is held about them. People like to know who is collecting information about them, what information is being collected and why. They want to feel confident that the information will not end up being used for a purpose that they did not expect. They also like to know that information about them is able to be corrected if it is incorrect.

A recent survey conducted by MasterCard makes clear that privacy is an important social issue to a significant proportion of Australians, ranking only just behind unemployment, the environment and law and order, and ahead of the national debt. The greatest concern related to financial information – banking, major purchases and income.

Consumer trust and loyalty are imperative to good business. That trust and loyalty can be destroyed if personal information of customers is misused or consumers fear that it may be misused. Let me translate this statement into a practical example. The MasterCard survey found that a significant segment of the population would discontinue a financial transaction for goods or services if personal information was sought during the transaction which they felt was unnecessary. The survey found that over a quarter of the adult public claims to have actually discontinued a financial transaction for this reason.

Advances in technology have particularly raised concerns about privacy. These advances have greatly enhanced the ability to collect and store data and to collate and use this data for different purposes. The capacity to store and reuse personal information has been of great benefit to business and has led to significant improvements in service delivery in many areas. You would be well aware of how these advances have enhanced service delivery in the banking industry. And we are only at the beginning of the opportunities which information technologies offer.

If privacy is inadequately protected in the new information technology environment, the confidence of users and potential users of such technologies and related services may be undermined, preventing optimal use of these technologies and services. Clearly this is not in the interests of those businesses seeking to utilise these technologies in service delivery – and banks are one of the key players in this respect.

So it is in the interests of business to address these consumer concerns. It is also in the interests of consumers that this is achieved without imposing unnecessary burdens and constraints on business. Such burdens and constraints inevitably translate into additional costs which are passed on to consumers.

There are avenues for a voluntary code of privacy protection in the private sector that safeguards both consumers and business.

As most of you would be aware from your banking connections, a number of sectors have already developed privacy principles. The Australian Bankers' Association Code of Banking Practice includes some privacy principles. The Credit Union and Building Society codes of practice contain similar principles. As well, Fly Buys, Visa and American Express also have privacy policies. Most recently, the Asia-Pacific Smart Card Forum – which is a body established by a group of companies with an interest in promoting the Australian Smart Card Industry – has developed a Smart Card Industry Code of Conduct which focuses mainly on privacy.

As I have indicated, the Prime Minister's announcement included the announcement that the services of the Privacy Commissioner would be made available to assist business in the development of voluntary codes and to meet privacy standards.

One approach to developing a voluntary approach to privacy protection in the private sector would be to continue to develop such codes for particular sectors or to cover particular functions. Alternatively, one overall set of privacy principles appropriate for application across the entire private sector might be developed.

If the first approach – an incremental approach – were to be pursued, there are advantages in pursuing functional, rather than sectoral, codes. By functional codes, I mean codes applying to a particular type of information or particular use of information – rather than focusing on who the code applies to. As the Wallis Financial System Inquiry Report shows – sectors are not fixed. Functional codes are better suited to having continued relevance to an evolving private sector.

From the consumer's point of view, a functional approach provides assurance that the same protections will apply, no matter who is providing the relevant good or service, or handling the particular type of information. From the business point of view, a functional approach provides a better basis for ensuring that there are no distortionary impacts on business competition.

The second approach – an overall set of privacy principles – might be an even better approach, at least as a first step. This approach would provide a uniform privacy standard across the entire private sector. Consumers could expect the same essential privacy protection in relation to all dealings with the private sector. Business would know that all players – even indirect competitors – would be playing by the same rules.

Such an overall set of privacy principles would also provide a basic starting point should the development of more detailed codes, specifically addressing issues relevant to particular types of information or functions, later prove desirable.

This overall approach has been taken in Canada. Under the auspices of the Canadian Standards Association, a committee developed a Model Code for the Protection of Personal Information. The committee was made up of a wide range of business, consumer and government representatives. It included, for example: the Canadian Bankers' Association; insurance groups; the Canadian Direct Marketing Association; communications and information technology groups; consumer groups, such as the Consumers' Association of Canada and the Public Interest Advocacy Centre; federal and provincial Privacy Commissioners; and the federal Justice and Industry Departments.

The Model Code was approved by the Canadian Standards Council as a National Standard in December 1995. More recently, the Canadian Standards Association has proposed to the International Standards Organisation that it develop an international standard on privacy. Should the International Standards Association proceed with this proposal, consideration would need to be given to whether the development of a voluntary approach in Australia should link in to this process.

Both our domestic experience to date in developing sectoral and functional codes and the Canadian experience must be taken into account in our pursuit of a voluntary approach to privacy protection in our private sector.

The Privacy Commissioner is currently meeting with business and consumer groups to discuss how she might facilitate the best voluntary approach to privacy for Australia at this point in time. I encourage you to make your views known to the Privacy Commissioner.

Whichever approach is followed, any codes developed will need to reflect the essential privacy principles. And there are a number of sources that we can look to in identifying these principles. The OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data which were adopted in 1980 are a starting point for many of the subsequent treaties, legislation and voluntary codes. These Guidelines are expressed in very general terms, as is appropriate for international guidelines, and they require fleshing out for actual implementation at the domestic level.

The Australian Federal Privacy Act does just that. It fleshes out these guidelines to set standards for the Federal Government, as well as in relation to tax file numbers and consumer credit reporting. The New Zealand Privacy Act similarly develops these principles for application to the New Zealand public and private sectors. The Canadian Standards Association also used the OECD Guidelines as the basis for the development of its Model Code.

The European Union Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data – which has attracted some press coverage lately – reflects the same essential principles.

I turn now to the principles themselves. Put very simply, they come down to individuals having control of their personal information.

Transparency is an important component. All current statements of these principles tackle provision for control and transparency by looking at each stage of the information handling process.

In the first stage of information collection all statements of privacy principles make clear that individuals should know why information is being collected – what it will be used for and who it will be disclosed to. And that only relevant information should be collected.

Privacy principles covering the use of that information make clear that personal information should only be used for the purposes for which it was collected, unless the person concerned consents to some other use.

Personal information should not be disclosed to third parties that the person concerned did not expect it to be disclosed to, without the consent of that person.

And finally, individuals should be able to know what information is held about them, and have it corrected if it is not correct.

That is a very brief explanation of the principles. They are more fully explained in the various national and international instruments that I have referred to. I have put the principles as general propositions. Privacy, however, is not an absolute. Competing public interests must be taken into account. There are exceptions and modifications to these general propositions needed to accommodate these other public interests.

Apart from the content of the principles to be set down in any code, consideration will need to be given to whether there would be any mechanisms for redress. Would an individual who felt that an organisation had not complied with a code be able to take any action? Would there be a person within the organisation to whom they could direct a complaint? Would there be an independent body to whom they could turn if they were not satisfied with the response of the organisation?

There are of course many existing industry complaint bodies, as well as the current role of the Privacy Commissioner in relation to the federal public sector and the credit reporting industry, to which we can look in seeking models for answering these questions.

The European Union Directive and the issue of State legislation are also pertinent to a voluntary approach to privacy protection in the private sector.

The European Union Directive – which EU countries are required to implement by 24 October 1998 – sets uniform privacy standards for all EU countries. It has two aims: to ensure the protection of the privacy of individuals within EU countries; and to ensure that information flows between EU countries will not be impeded by the existence of differing standards of protection in EU countries. It covers information held by both the public and private sectors. As I have indicated, the privacy standards set down by the Directive reflect the essential privacy standards found in other international and national instruments. They set standards for collection, storage, use, disclosure, access and correction.

In addition, the Directive regulates transfers of personal information from EU countries to non-EU countries. It aims to ensure that the privacy protections covering EU countries are not undermined by the transfer of personal information to countries without such privacy protections. Questions have been raised in the media about the potential impact of the Directive on Australian trade with EU countries. As a general starting point the Directive requires member countries to provide that the transfer of personal information to non-EU countries may take place only if the non-EU country "ensures an adequate level of protection".

You may well ask, "what constitutes adequate level of protection?" The Directive states that "the adequacy of the level of protection" is to be "assessed in light of all the circumstances surrounding a data transfer operation or a set of data transfer operations" and that "particular consideration" is to be given to: "the nature of the data, the purpose and duration of the proposed processing operation or operations, the rules of law, both general and sectoral, in force in the [non-EU country] and the professional rules and security measures which are complied with in that country". So it is clear that case by case assessments can be made.

The criteria against which those assessments would be made is less clear.

Presumably the protections set down in the Directive for application within EU countries provide some guidance, but it is important to note that the Directive does not require identical protections. It does not even require equivalent protections. The term used is "an adequate level of protection". This choice or wording represents a specific rejection during the development of the Directive of suggestions that the term "equivalent" should be used. We understand that the European Commission has engaged an expert to advise on a methodology to determine what is an "adequate level of protection". The Australian Government is maintaining contact with the European Commission on developments.

However, the issue of information flows from EU countries to Australia will not turn solely on the question of "adequate" protection. Even where a non-EU country does not ensure an "adequate level of protection", the Directive permits transfers in a number of circumstances. I shall mention those that would be of particular relevance to business.

The first is where the person concerned has given their unambiguous consent to the proposed transfer. Where the person concerned knows that their information is to be transferred to a particular country, it is for them to decide whether they want the transfer to go ahead. Similarly, where a transfer is necessary for the performance of a contract with the person concerned or the implementation of pre-contractual measures in response to a request from the person concerned, there are no restrictions. This would cover cases such as banking transactions, airline booking information and other travel arrangements. Thirdly, transfers necessary to implement a contract concluded in the interests of the person concerned may take place regardless of "adequacy". In all of these cases, the information transfer can go ahead automatically without any consideration needing to be given to "adequacy".

In addition, and perhaps most importantly, the Directive allows EU countries to authorise a transfer, or a set of transfers, of personal information to a country which does not ensure an "adequate level of protection" if there are "adequate safeguards". The Directive specifically states that such safeguards may result from appropriate contractual clauses.

It envisages that the European Commission might draw up standard contractual clauses which would constitute "adequate safeguards". So, even if a country is considered not to have an adequate level of privacy protection, and a particular transfer of personal information does not fall within the specific circumstances that I have mentioned, the relevant EU country can allow a transfer on the basis of appropriate contractual requirements that privacy be protected.

In summary, while trade with Europe is clearly very important to Australia, and constraints on that trade would be a matter of considerable concern, we should not assume that the implementation of the EU Directive will necessarily cause significant constraints. The Federal Government will continue to monitor this issue closely.

I turn now to the issue of State legislation. Concerns about the growing potential for a patchwork of State privacy laws emerged during the consultations on the discussion paper.

Business is increasingly operating nationally. Being required to comply with a range of differing, if not inconsistent, privacy regulations, would have implications for the costs and efficiency of business.

These concerns are well understood by the Government. I have pressed it in discussions with my State counterparts in the Standing Committee of Attorneys-General. The Prime Minister has raised it directly with State Premiers in their meeting on 21 March 1997.

At that meeting, the Prime Minister asked the Premiers and Chief Ministers not to introduce privacy legislation within their own jurisdictions. Both the Northern Territory and Queensland responded by agreeing not to introduce such legislation. Other States indicated that they would consider the Commonwealth's request. The Prime Minister also followed up by putting this request to the States in writing. This action by the Prime Minister demonstrates the Government's commitment to avoiding unnecessary burdens being placed on business.

However, while the Government believes that blanket application of the Privacy Act to the private sector is not appropriate, the Government will act where necessary to maintain the status quo in relation to information collected for the purposes of Government.

The Government has recently decided, in the context of consideration of the government's information technology infrastructure, that we will legislate to extend the application of the Privacy Act to cover contractors supplying services to government in relation to personal information held on behalf of the government. This move will ensure that the current protections of the Privacy Act will continue to apply when personal information currently held by the government is transferred to a private sector body as part of such outsourcing. Australians have a right to expect that, when their information is held on behalf of the government, it will be subject to appropriate protections regardless of whether it is held by a public servant or a private sector contractor.

In conclusion, can I say that in relation to privacy protection in the private sector generally, we believe that a voluntary approach is the way ahead to ensure nationally consistent privacy protections which provide the protections consumers want while not imposing unnecessary burdens or constraints on business. With Government and business working together on improving the level of privacy protection in Australia I believe that Australians will continue to be assured that their privacy is well protected.