ATTORNEY-GENERAL'S DEPARTMENT

Information and
Security Law Division

The Australian Approach to Privacy Protection in the Private Sector

World Intellectual Property Organization (WIPO)
Second International Conference on Electronic Commerce
and Intellectual Property
21 September 2001

Presentation by
Ms Helen Daniels
Assistant Secretary
Information and Security Law Division
Commonwealth Attorney-General's Department
Australia

Introduction

New technologies are presenting new challenges and, as a result, it is necessary to re-evaluate the way we do things.

New technologies do, for example, raise real concerns about security, authentication and privacy.

The privacy challenges faced by organisations in the paper-based environment have been largely superseded by those posed by the ever changing information technology environment.
The use of the Internet raises particular concerns about privacy because of the ease and speed with which personal information can be collected, stored and disseminated.
Organisations that ignore privacy issues do so at their own peril.
Some companies have found out through hard experience, that where they disregard the privacy of their customers they pay a high price in terms of adverse media coverage, loss of business and plummeting share value.
But the situation is even more serious than that.
Left unaddressed, concerns about privacy could potentially threaten the development of electronic commerce and the information economy.
Smart businesses and other organisations that handle personal information are already moving to address issues of privacy.
They have put in place privacy codes of practice in recognition of the commercial advantages to be gained from good privacy practices.
However, these organisations are still in the minority. Surveys on Internet privacy show that, in the electronic environment at least, many private sector organisations in Australia have a long way to go.
The Australian Government recognises that it has a critical role to play in supporting business and the continued development of electronic commerce and the information economy generally.
A key part of the Australian Government's legal and regulatory framework put in place to encourage development in these areas is the *Privacy Amendment (Private Sector) Act 2000* or what is known as the private sector privacy legislation. This legislation passed through the Parliament in December 2000 and will come into effect for many organisations from 21 December 2001.
I am pleased to be here today to talk to you about the new legislation and its implementation in Australia.
Of course, privacy regulation is not new in the Australian environment. The Commonwealth public sector has been regulated by the *Privacy Act 1988* since 1 January 1989. The legislation protects the personal information of individuals held by public sector agencies. It also regulates the information privacy aspects of the consumer credit reporting and makes provision for the Federal Privacy Commissioner to issue Tax File Number Guidelines.
The legislation also establishes the statutory office of the Federal Privacy Commissioner. The Commissioner is the independent regulator for privacy at the national level. His office is presently staffed by about 40 people.

Private Sector Privacy Legislation

The Australian Commonwealth Government was committed to enacting balanced privacy legislation for the private sector to ensure that full advantage could be taken of opportunities that electronic commerce presents for Australian business within Australia

and overseas. A country that could demonstrate it protects its citizens' privacy would have an advantage over those that countries that do not.
The *Privacy Amendment (Private Sector) Act 2000* is intended to create a more level playing field for business and other private sector organisations by providing minimum rules for the handling of personal information.
It has been the subject of an extensive consultation process with business, consumer and privacy stakeholders over a number of years. The legislation built on self-regulatory principles that the then Privacy Commissioner had developed following consultation with business in 1998.
The legislation has been developed with international standards, such as the OECD data protection principles and the European Union Directive on personal data protection, in mind.
It is designed to assist Australian business in the international marketplace and be of particular benefit to our trade with the European Union Member States.

The legislation is co-regulatory

Far from being heavy-handed, the legislation meets the Australian Government's commitment to promote a light touch, co-regulatory approach to privacy protection. It is also technology-neutral in its application. This avoids the need for constant revision as technology evolves.
The legislation is not overly prescriptive.
The Australian Government is of the view that it is far better for business and industry to cooperatively embrace good privacy practices by appreciating the benefits that flow from respecting the personal information they handle than for the Government to impose a heavy-handed regime.
The co-regulatory approach adopted represents a workable middle ground between over prescription and self-regulation.
A key feature of the co-regulatory approach enables organisations to develop their own privacy codes regulating the collection, storage, use and disclosure of personal information.
The National Privacy Principles, which I shall discuss in more detail, provide minimum benchmarks for the development of privacy codes under the legislation.
Private sector organisations are, however, free to adopt higher standards if they consider it appropriate to their circumstances. Any code developed must meet certain prescribed standards and be approved by the Federal Privacy Commissioner.
The National Privacy Principles will operate by default where a business or other organisation chooses not to develop its own privacy code, or is not covered by a code that has been approved by the Federal Privacy Commissioner.

The legislation regulates "organisations"

The legislation regulates the acts and practices of "organisations".
An organisation is defined to mean a body corporate, an unincorporated association, a partnership, a trust or an individual. Therefore an organisation does not need to be 'for profit' to be covered by the legislation – there is no distinction between commercial and non-commercial organisations.
However, the legislation will not apply to small business operators or registered political parties. The acts and practices of media organisations done in the course of journalism will also be exempt.
Employers dealing with personal information on employee records are exempt in certain circumstances. This exemption is obviously very relevant in the workplace context.

The legislation protects "personal information" contained in "records"

The legislation provides standards for handling individuals' *personal information* collected, and contained in *records* held, by organisations.
Personal information basically comprises any information or opinions about an individual from which their identity is apparent or can reasonably be ascertained.
A *record* includes a document, database or photograph, or other pictorial representation of a person.
This will include, for example, personal information collected and recorded on websites and through optical surveillance and similar devices.

National Privacy Principles set the standards for handling personal information

The standards for handling personal information are contained in ten principles, known as the National Privacy Principles.
These principles are based on the *National Principles for the Fair Handling of Personal Information*, which were developed by the Federal Privacy Commissioner.

The National Privacy Principles regulate the

- collection; (NPP 1 and 10)
- use and disclosure; (NPP 2) and
- transfer overseas (NPP 9)

of personal information.

They require organisations to ensure that the personal information they hold is

- accurate, up-to-date and complete; (NPP 3) and
- secure (NPP 4).

Organisations are also required to

- be open about how they manage personal information; (NPP 5);
- provide access and correction rights to individuals; (NPP 6) and
- allow people to deal with them anonymously, if that is legal and practical (NPP8).

The National Privacy Principles also

- prohibit the use of Commonwealth Government identifiers; (NPP7).

The legislation extends additional protection to health information

The legislation provides additional protection in relation to the use and disclosure of health information.
NPP 10 limits the ways that sensitive information, including health information, may be collected. ('Sensitive information' also includes information or an opinion about an individual's racial or ethnic origin; political opinions; membership of a political association; religious beliefs or affiliations; philosophical beliefs; membership of a professional or trade association; membership of a trade union; sexual preferences or practices; or criminal record.)
As a further example of how health information is protected at a higher level, National Privacy Principle 2 prohibits the use of sensitive information, such as health information, for direct marketing purposes.

Small business exemption

The Australian Government is committed to cutting red tape and minimising the compliance burden placed on business by regulatory regimes.
This policy is reflected in the legislation through the inclusion of an exemption for small business operators.
A small business is one with an annual turnover of Aus $3 million dollars or less.
The exemption recognises that the vast majority of small businesses do not hold an extensive amount of personal information and therefore pose a low risk to privacy.
But not all small businesses are able to take advantage of the exemption.
Small businesses that pose a higher risk to privacy will be brought within the legislation - namely, small businesses that provide health services and hold health information; trade in personal information; or are contracted to provide a service to a Commonwealth Government agency. There is also a mechanism for a small business to 'opt-in' to the privacy scheme through inclusion in a register with the Federal Privacy Commissioner.

The legislation will not apply to employee records in most circumstances

In most cases, the legislation will not regulate how employers handle employee records.
This is because the Australian Government is of the view that the regulation of employee records is an area that is better dealt with in the context of workplace relations reform rather than privacy regulation.
The legislation provides that an act done, or practice engaged in, by an employer is exempt

from the operation of the legislation if the act or practice is directly related to:

- a current or former relationship between the employer and the individual; and
- an employee record held by the employer relating to the individual.

The Federal Privacy Commissioner will play a major role

The Federal Privacy Commissioner, Mr Malcolm Crompton, will be a key player in the implementation of this legislation.
Part of the role of his office will be to help people understand and accept the National Privacy Principles and to help organisations to develop their own privacy codes. His office is releasing practical guidelines on the National Privacy Principles, Health Information and the Development of Codes. There are also information sheets and checklists available from the website of his Office.
As privacy codes are developed, the Commissioner will also be responsible for their approval.
Some organisations such as the Internet Industry Association have already taken steps to prepare their code. The code includes standards that go beyond the minimum standards of the legislation.
One further role the Commissioner will play is that of an adjudicator in the resolution of complaints.

Making a complaint is simple

The complaint-handling process will enable people to have their complaints dealt with simply, quickly and at low cost.
It is designed to ensure that most complaints can be resolved through conciliation and mediation, rather than through an adversarial court process.
The stage of conciliation is based on accepted principles of alternative dispute resolution. In most cases, this would involve phone calls and letters to the parties. In a small proportion of more intractable matters, meetings with the parties face to face would be necessary.
Where the organisation has a privacy code and a mechanism for handling complaints, the independent investigator will be the adjudicator nominated under the code.
In those instances where an organisation does not have a complaint handling mechanism, the complaint will be handled by the Federal Privacy Commissioner.

There is also an appeal mechanism from a decision of a code adjudicator to the Privacy Commissioner if an individual is not satisfied.

Remedies if a complaint is made out

When the Federal Privacy Commissioner or a code adjudicator determines that an organisation has interfered with a person's privacy, they can do one of several things. These include:

- declaring the organisation should not repeat or continue the offending conduct;
- requesting the organisation to redress the loss or damage suffered by the person concerned; and
- requesting that the organisation pay compensation for any loss or damage suffered by the person.

"Loss or damage" can include injury to the person's feelings or any humiliation suffered by that person.

Of course, often the simple act of “naming and shaming” an organisation should provide an adequate incentive for the organisation to improve its privacy practices and procedures. Only twice in the twelve year life of the Privacy Act has the Commissioner had to use the formal determination making powers under the Act and one of these occasions was at the request of the respondent.

If the parties do not comply with the terms of a determination, the Act allows the Privacy Commissioner to approach the Federal Court or the Federal Magistrates Service to seek enforcement through a de novo hearing.

The Privacy Commissioner also has powers to seek injunctions to ensure compliance with the Act. Again, these powers have never been used to date.

I will now turn to outline a couple of the key National Privacy Principles in the legislation.

Collection of personal information needs to be fair

The National Privacy Principles regulate how and when an organisation can collect personal information.
Personal information must be collected in a fair and lawful way.
This means that the organisation must tell their customers or clients that they are collecting information about them.
Organisations should collect personal information directly from the individual to whom the information relates and should tell them how their personal information will be used and to whom it will be disclosed.
Under the legislation, organisations that collect personal information through a website will have to take reasonable steps to ensure that the individual knows who is collecting the information, why it is being collected, what will be done with it and so on.
In practice, this will mean that all websites will have to include a clearly identified privacy statement.
The purpose of a privacy statement is to inform people about how their personal information will be handled.
There are privacy enhancing technologies and tools available to assist organisations come to terms with good privacy requirements and practices. For example, the privacy policy statement generator released by the OECD[1] is a useful tool.
The generator takes the form of an interactive questionnaire that can be used to develop a privacy policy statement.

There are restrictions on the use and disclosure of personal information

The private sector legislation will also restrict what organisations can do with personal information after it has been collected.
The general rule in the National Privacy Principles is that personal information should only be used or disclosed in a way that is consistent with people's expectations, or where it is in the public interest to use it or disclose it in that way.
An organisation that collects personal information for one purpose cannot automatically use or disclose it for another purpose.
For example, personal information provided for the purpose of subscribing to a particular publication or mailing list, cannot be used for direct marketing purposes unless certain conditions are met.
The legislation will allow the use of personal information for the secondary purpose of direct marketing, provided the individual is given the opportunity to "opt-out" of receiving any further direct marketing communications.

Personal information must be stored securely

Once an organisation has collected personal information, the National Privacy Principles will require that reasonable steps are taken to protect personal information from unauthorised access and disclosure.
Website operators who handle personal information will have to address issues of data security, such as encryption and authentication.

Individuals have a right to access and correct their personal information

The National Privacy Principles will also give individuals the right to access most records containing personal information about them, and to seek to have those records corrected if they are wrong.
Organisations will need to consider how requests for access will be lodged and how access

[1] the privacy policy generator is available on the OECD home page at: http://www.oecd.org

will be granted.
If access is granted electronically, then the organisation will also need to consider issues of encryption and authentication.

Concluding comments

The Federal Privacy Commissioner's website provides useful guidance on Australia's new law and I commend it to you[2].

New technology in particular has heightened our awareness of privacy issues.

With this heightened awareness comes an expectation that we should have some say about when our personal information is collected, how it will be used, and where it will end up.

Customers and clients expect business to respect their privacy, and businesses that fall short of the mark will suffer the consequences.

Privacy is clearly not just a passing fad.

Like other issues where society has demanded new standards, such as in the human rights area, privacy protection in some form is here to stay.

The approach in the *Privacy Amendment (Private Sector) Act 2000* is the Australian Government's way of providing business and other organisations with an opportunity to take responsibility for developing their own good privacy practices and at the same time ensuring individual's personal information is protected in an appropriate way.

[2] the Privacy Commissioner's home page is at: http://www.privacy.gov.au