Developments in privacy since 21 December 2001

*Catherine Rowe and Lisa Ritchie, Freehills**

Catherine Rowe is a solicitor at Freehills working in the Corporate practice group. Catherine advises on privacy, commercial and technology issues. Lisa Ritchie is a Graduate at Law at Freehills working in the Corporate practice group.
This paper is based on a presentation given at a seminar held by the New South Wales Society for Computers and the Law in June 2002.

> "The fantastic advances in the field of communication constitute a grave danger to the privacy of the individual."
>
> Earl Warren (1891-1974)
> US Supreme Court Chief Justice

1 Overview: the information age and the need for privacy legislation

As most people are now aware, new provisions in the Privacy Act 1988 (Cth) (**Privacy Act**) came into effect on 21 December 2001, which regulate the collection, use, disclosure, quality and security of personal information in the private sector.

Privacy laws and data protection laws have become increasingly important in recent years. The development of information technology and e-commerce has dramatically increased the quantity of information available in digital form and the ways in which it may be collected and communicated in a global commercial forum.

In this information age, information is a valuable commodity, and databases are being sold and licensed at high prices. As technophobes and technology-lovers alike became concerned about these intrusions into their 'personal cyberspace', privacy legislation became essential to ensure that individuals could retain control over how their personal information is dealt with.

This article examines some of the developments in privacy since the new provisions in the Privacy Act came into effect.

2 The increasing public consciousness of privacy

In the nine months since the Privacy Act came into effect, the Office of the Federal Privacy Commissioner (**OFPC**) has changed its approach from informing organisations of their privacy obligations to educating consumers about their 'right' to control the collection, use and disclosure of their personal information. It has released a brochure called 'My Privacy -- My Choice'[1], which formed part of a national privacy campaign with advertisements in major Australian newspapers.

Indeed, there is evidence that consumers are already exercising their privacy rights. The OFPC stated in a June media release that that there has been a threefold increase in calls to the OFPC Privacy Hotline compared to the six months before the Privacy Act came into effect.[2] The media release also stated that 456 written privacy complaints were lodged with the OFPC between December 2001 and June 2002, which primarily related to:

- getting access to personal information;
- unnecessary collection of information;
- use of personal information for direct marketing and the lack of 'opt out' provisions;
- improper disclosure of personal information; and
- broadly drafted disclosure consent forms which only allow a single consent to all forms of disclosure.

All indicators suggest that the public are becoming increasingly privacy conscious, and that businesses which fail to implement privacy compliant business practices risk exposure to complaints and may find themselves subject to OFPC scrutiny. In this regard, one commentator has stated that an organisation must have a 'culture of privacy awareness' to ensure complete and sustained compliance with the Privacy Act.[3]

3 The Australian privacy landscape

There have been interesting and unexpected developments in privacy in both the commercial sector and the community since the Privacy Act came into operation.

It has been reported that a privacy audit undertaken by Aulich & Co. into a range of industries revealed that airlines, banks, insurance companies and IT companies in particular have failed to implement privacy compliant business practices.[4] Responding to the Aulich report, a spokeswoman for the OFPC commented that the government would consider the introduction of tougher penalties when it reviews the privacy legislation in 2003:

> "This is the minimal level of privacy compliance Australian companies will ever face, so they need to make it work to avoid tougher laws."[5]

The Aulich report cited customer loyalty programs such as frequent flier programs as a particular problem area, as they collect credit and personal information which is subsequently used for a variety of purposes.

3.1 Bundled consents

It has been reported that the OFPC is currently investigating some of Australia's largest and most powerful corporations over their privacy policies.[6] It has received a large number of complaints over broad privacy policies which effectively indicate that the company will not continue to provide the individual with its services unless they agree to the broad use and disclosure of their personal information. The OFPC commented on this issue in a media release in May:

> "Bundled consents are not good privacy or business practices and

are totally contrary to the spirit of the Privacy Act."[7]

Firstly, bundled consents diminish an individual's freedom of choice by inducing them to hand over their valuable personal information in exchange for a service. Secondly, individuals are asked to consent to a number of unrelated, often intrusive, information handling practices as a condition of receiving this service.

The media release flagged the issue of bundled consents as a potential matter for consideration in the OFPC review of the Privacy Act in 2003.

3.2 Football

Privacy issues and myths have arisen in the general community as well as in large commercial organisations. For example, in an article called 'Ridiculous law silences coaches'[8], the Queensland *Courier Mail* reported that sports coaches may breach privacy laws by speaking publicly about player injuries. However, the OFPC has clarified this issue on its website, stating that a sports club may disclose information about a player's injuries so long as the player understands that this is likely to happen and has consented to it.[9]

3.3 Church

Privacy has even intruded into the spiritual sphere.

Concerns arose in the church community that the practice of public prayers or printing of personal information in church newsletters would be a breach of the Privacy Act. However, the OFPC stated in a media release in May this year that this use of personal information would not breach the Privacy Act, as these practices would be within people's reasonable expectations so long as the church has a clear privacy policy about its use of members' personal information and members are made aware of church practices when they join the congregation.[10]

Clearly, all sectors of the community are grappling with the new right to privacy.

3.4 Industry privacy codes

Under section 18BA of the Privacy Act, an organisation or industry association may apply to the OFPC for the approval of a privacy code. Once approved, the organisation's privacy code (or the industry privacy code to which it is bound) will replace its obligations under the National Privacy Principles (**NPPs**).

The OFPC approved Australia's first private sector privacy code in April this year, the General Insurance Information Privacy Code (**Insurance Privacy Code**)[11] submitted by the Insurance Council of Australia. The Insurance Privacy Code will bind organisations which sign the 'General Insurance Information Privacy Code Deed of Adoption'.

The privacy obligations under the General Insurance Information Privacy Principles (**GIIPPs**) and the NPPs are identical in substance. However, in addition to complying with the GIIPPs, an insurance organisation which is bound by the Insurance Privacy Code must implement a complaints handling scheme in accordance with the Code and will be subject to periodic compliance monitoring by Insurance Enquiries and Complaints Ltd.

The OFPC has also recently approved the Queensland Club Industry Privacy Code.[12]

3.5 Online medical records

Another issue which has attracted publicity in Australia is the privacy issues raised by the integrated storage of medical records. If this occurs, doctors and health care practitioners would be able to access a centralised database which would contain a comprehensive record of a person's medical history, prescribed drugs or allergies.

There are increasing numbers of proposals for the linkage of identified medical records, for example, 'Telemedicine' and 'health smart cards'. The HealthConnect network is currently being investigated by the Commonwealth government in partnership with the States and Territories. It is a voluntary scheme to enable the electronic collection, storage and exchange of health information with strict privacy safeguards. It has been reported that trials will begin in the Northern Territory and Tasmania by the end of this month, to be followed by trials in NSW and Queensland late next year.[13]

Of course, under the NPPs, health information is considered 'sensitive information' and subject to tighter controls. In addition, some states have enacted specific privacy legislation which is focussed particularly on health information such as the Health Records Act 2001 (Vic) and the Health Records (Access and Privacy) Act 1997 (ACT). The Health Records Information Privacy Act 2002 (NSW) was recently assented to. It aims (among other things) to provide for an integrated electronic health system within NSW. Under the Bill, express consent from an individual is needed for their health information to be linked to an electronic health record.

Critics of the electronic storage of medical records argue that the records would be vulnerable to unauthorised access and there are fears that patient information would be sold to pharmaceutical companies for market research purposes.

On the other hand, integrated online medical records would have tangible benefits. It would give doctors a systematic and comprehensive patient medical history. For example, it could avoid 'medical misadventure' as a consequence of dangerous drug interactions caused by doctors acting without the right information.

The implementation of integrated electronic medical records will require a careful consideration of consumer, public and private interests.

4 Getting it wrong – privacy and trade practices

Businesses, politicians and the media have often emphasised the 'soft touch' approach of the Privacy Act. However, it is clear that organisations should not underestimate the potential legal consequences of breaching their privacy obligations.

A privacy policy which inaccurately or incompletely describes a

company's information handling practices may not only breach the Privacy Act, but may also amount to misleading or deceptive conduct under the Trade Practices Act 1974 (Cth) (**Trade Practices Act**).

The Australian Competition and Consumer Commission (**ACCC**) and the OFPC signed a memorandum of understanding earlier this year which stated their intention to cooperate in privacy enforcement, investigations, litigation, training and education.[14] In particular, they will work together to ensure that privacy policies issued by companies are not misleading or deceptive under section 52 of the Trade Practices Act. As one media article commented, "the Privacy Commissioner has got himself a pair of boots".

The Chairman of the ACCC, Allan Fels, has indicated that the ACCC and the OFPC may conduct a 'joint internet sweep day' which targets online privacy compliance.[15] The last internet sweep by the ACCC conducted in September 2001 revealed that only 27 per cent of Australian e-tailers had posted a privacy notice.

While many organisations have now posted some sort of privacy notice on their website, it has been reported that organisations are surfing the internet to locate privacy policies and cutting and pasting them onto their own website. Any organisation which publishes a privacy policy that bears no resemblance to the company's actual handling of personal information will risk liability for misleading and deceptive conduct.

5 E-commerce issues – privacy policies

This article has already discussed how much of the need for privacy has arisen out of developments in e-commerce and information technology. It has been estimated that 18 billion dollars worth of e-commerce would be lost this year as a consequence of consumer distrust in the current privacy environment.[16]

Until privacy concerns are addressed, e-commerce will be hindered. Privacy policies can go a long way to alleviating privacy fears and promoting e-commerce.

5.1 Privacy policies and NPP 1.3 collection notices

Although the Privacy Act does not require an organisation to have a website privacy policy, it is considered good practice to do so. A notice under NPP 1.3 should be posted on a website if it collects personal information. This notice will need to explain (among other things) the identity of the organisation and the types of organisations to which it usually discloses personal information.

It is essential for organisations to ensure that their specialist on-line service providers (for example, web-hosts) are consulted when the website privacy policy and NPP 1.3 collection notice are drafted and reviewed, since it is often only these organisations that fully comprehend how personal information is collected and handled on the website. For example, many organisations merely receive a monthly report from their web-host which indicates how many visitors have visited the site. However, the web-host or internet service provider (**ISP**) may often collect and process far more personal information about individuals' activities on a particular website.

The process of reviewing a website privacy policy and NPP 1.3 collection notice should therefore involve liaison between a variety of stakeholders including the technical and commercial staff responsible for the website, the areas of the organisation using the personal information and relevant third party service providers.

5.2 Cookies

Not all of the information collected by a website is personal information. For example, some information may merely be the visitor's internet protocol (**IP**) server address or domain name, from which an individual's identity cannot be ascertained. However, other information collected may amount to personal information. For example, if an individual's email address contains their full name, it may be used as a means of identification and is therefore personal information.

While cookies may merely recognise a computer's IP address, once this information is linked with other personal information that is collected on a website (for example, an email address that contains a person's name or personal information voluntarily provided when an individual registers on the website), then cookie information may amount to personal information. As noted in the Guidelines to the National Privacy Principles (**NPP Guidelines**):

> "If an organisation collects personal information using a cookie, web bug or other means, it could give the NPP 1.3 information in a statement clearly available on the web site."[17]

5.3 Changes to privacy policies

Privacy advocates are becoming increasingly disgruntled by a perceived tendency for companies to unilaterally change their privacy policy to the detriment of consumers. For example, in March, Yahoo changed its users' preferences to 'yes' in relation to the receipt of marketing material, forcing members to 're-opt out' of receiving marketing communications from the company about various products.[18]

5.4 US legislative developments – online privacy

The US Senate Commerce Committee has approved two bills, which will now be debated by the full Senate.

The Online Personal Privacy Bill 2002 requires internet service providers and commercial Websites to get customers' explicit consent before they may collect, use or disclose sensitive information. Companies must also give individuals the opportunity to 'opt out' of further communications when it collects non-sensitive information. The bill allows consumers to sue companies that mishandle their personal data.

The Controlling the Assault of Non-Solicited Pornography and Marketing Bill 2001 requires companies to include a working return email address to allow recipients to refuse further communications from the company. It also gives internet service providers

the ability to keep spam out of their networks, prohibits companies from transmitting unwanted e-mails to addresses that were illegally obtained from websites and gives the Federal Trade Commission the authority to impose fines of up to $10 per e-mail violation with a cap of $500,000.

5.5 Spam Prevention Early Warning System (SPEWS)

Given the media and public focus on spamming, it is interesting to note that a Perth marketing firm is taking action against an individual for sending an unfounded complaint to the Spam Prevention Early Warning System (**SPEWS**), an anti-spam website which black-lists IP numbers believed to be used for unsolicited bulk email or spam.[19]

Network administrators and ISPs who subscribe to SPEWS block traffic to and from the black-listed IP addresses. The plaintiff marketing company is arguing that the black-listing disrupted its business and prevented it from sending emails to or on behalf of its clients.

6 International privacy laws

Worldwide privacy and data-protection laws have been particularly challenging for:

(a) multinational organisations whose businesses are reliant upon personal data being transferred worldwide; and

(b) e-commerce organisations for whom the multi-jurisdictional transfer of data is central to their business model.

Following is a brief exploration of some of the key issues facing these organisations and options for compliance with the transborder dataflow restrictions in different jurisdictions.

6.1 European Union - Data Protection Directive

The most significant transborder dataflow restrictions are contained in European Union Data Protection Directive 95/46/EC (**EU Directive**). The EU Directive allows European Union member states to legislate to protect EU citizens' personal information when it is handled by both public and private sector organisations.

Articles 25 and 26 of the EU Directive generally restrict the transfer of personal data to a country outside the European Union (**EU**) unless certain requirements are met, such as:

(a) the other country ensures an 'adequate' level of data protection;

(b) the parties have an appropriate contractual relationship; or

(c) the individual has given consent.

The EU Data Protection Working Party (**Working Party**) has concluded that the Australian Privacy Act does not provide an adequate level of protection, primarily because of the small business, employee records and direct marketing exceptions.

The Working Party has found that Canada, Switzerland and Hungary meet the 'adequacy' test.

6.2 United States - Safe Harbor scheme

The United States does not have privacy or data protection legislation of general application. Rather, it has ad hoc legislation relating to specific issues, such as health information and children's information. The US therefore does not have 'adequate' data protection laws for the purposes of the EU Directive.

One reaction to the EU Directive by companies in the US has been the development of a "Safe Harbor" scheme which was approved by the EU in July 2000. The Safe Harbor scheme is a self-regulatory scheme in which companies certify each year to the US Department of Commerce that they agree to comply with the Safe Harbor Privacy Principles, which impose requirements with respect to notice, choice, onward transfer, data integrity, access and enforcement. As a consequence, Safe Harbor companies have the degree of 'adequate protection' required to transfer data from the EU.

There are 2 ways of enforcement under the Safe Harbor scheme:

(a) self-regulation, whereby each company must have a dispute resolution system. The types of remedies for breach include a public statement or suspension of membership; and

(b) the Federal Trade Commission may bring an action on the basis of unfair and deceptive laws.

The take up of the Safe Harbor scheme has been less than explosive. However, its proponents remain optimistic for its success. Microsoft, Intel, Dun & Bradstreet and Hewlett Packard all signed up for the Safe Harbor scheme last year.

Many US companies have elected not to join the Safe Harbor scheme, preferring instead to enter into contracts with EU companies (or not to enter into contracts at all). Organisations have expressed concern that by joining the Safe Harbor scheme, they risk attracting the attention of the Federal Trade Commission.

6.3 Australia - NPP 9

NPP 9 of the Privacy Act restricts the transfer of personal information outside Australia without the consent of the individual concerned unless certain requirements are met. One of these is where the organisation has a reasonable belief that the organisation is subject to privacy laws or schemes that are substantially similar to the NPPs. It would generally be reasonable for Australian organisations to believe that the Safe Harbor Scheme and data protection laws in the EU, Canada, Switzerland and Hungary would not only be substantially similar, but may actually provide a higher level of privacy protection.

7 Transborder data flow

Transborder dataflow issues arise for all Australian organisations that either:

(a) transfer personal information to recipients that don't have substantially similar privacy protections; or

(b) receive personal information from companies in the EU or in other countries which have, themselves, restricted onward transfers.

7.1 Countries without substantially similar privacy laws

Recipients that do not have 'substantially similar' privacy protections are likely to be those in jurisdictions outside the EU, the Safe Harbor scheme, Canada, Switzerland and Hungary. Under NPP 9, an Australian organisation may only transfer personal information to such recipients in certain circumstances, including if they have the consent of the individuals or if they take "reasonable steps" to ensure the information will not be handled by the foreign entity in a manner which is inconsistent with the NPPs. 'Reasonable steps' will generally require that specific data protection clauses are incorporated into contracts with foreign entities to whom personal information is being transferred.

These clauses will impose obligations on the entity receiving the personal information to treat it in accordance with the NPPs. This has the effect of exporting the Privacy Act controls that apply in Australia with the personal data. The information therefore remains subject to these controls even though the processing of the data occurs in another jurisdiction which may be unregulated.

7.2 Receiving personal information from the EU

If an Australian organisation is receiving personal information from the EU, the EU organisation will be required to demonstrate that the level of protection afforded by the Australian entity is "adequate".

Given Australia's current "inadequacy rating" by the Working Party, in practice this means that unless the data subject has given consent to the transfer or any of the other exceptions under the EU Directive apply, the Australian entity will be required to agree to "EU model contract clauses" (**Model Clauses**). These Model Clauses have been drafted by the EU Commission and are recognised by all 15 member states as providing adequate safeguards for the protection of personal data. Under the Model Clauses, both the data exporter (in the EU) and the data importer (in the non-member country) undertake to process the data in accordance with basic data protection rules and agree that individuals may enforce their rights under the contract. Different sets of clauses exist for controller-to-controller transfers and for controller-to-processor transfers.

However, many Australian organisations are reluctant to agree to the Model Clauses as they impose burdensome requirements on data importers. Similarly, many US companies have also found the Model Clauses not to be a viable option, as they impose more stringent requirements on companies than the Safe Harbor scheme, such as limiting the use of data and imposing stricter access requirements.

Most significantly, the Model Clauses also give the individuals whose personal information is being transferred (the data subject) the right to enforce certain clauses in the agreement between the data exporter and the data importer. This raises privity of contract issues. The common law doctrine of privity of contract prevents third parties from enforcing the terms of a contract to which they are not a party. However, legislation in Queensland[20], Western Australia[21] and the Northern Territory[22] permits, in certain circumstances, a third party to enforce the terms of a contract to which they are not a party. The UK[23] and New Zealand[24] have similar legislation to redress these restrictions.

Despite the fact that laws enacted in accordance with the EU Directive sometimes contain penalties of both fines and criminal sanctions for a breach, there doesn't appear to be a great amount of pressure by EU organisations to ask their non-EU business partners to sign up to the Model Clauses. However, it appears that European authorities have not been aggressively enforcing their rules, even against businesses in their own countries. The lack of adoption of the Model Clauses is likely to be one of the key points for discussion at the recently announced EU review of the Directive.

Alternatively, the Australian organisation to which the EU organisation is transferring personal information may adopt a code of practice that satisfies the adequacy requirements of the EU Directive. For example, the Internet Industry Association has issued a draft Privacy Code which is in its final stages of review before being submitted to the OFPC for approval.[25] A key objective of the "European Extension" version of the draft IIA Privacy Code is to create a privacy regime that addresses the areas of "inadequacy" determined by the Working Party and thereby satisfy the transborder dataflow provisions in the EU Directive.

Once approved by the Privacy Commissioner, the IIA has stated that it will submit a copy to the Working Party for approval.

8 Privacy and surveillance

As well as increasing concerns about cybercrime and internet fraud, the events of 11 September 2001 have given rise to increasing calls for surveillance and monitoring in the interests of national security. Identity checking and tracking is being put forward by governments as an important weapon in response to the threat of terrorism.

Such calls imply that responding to this new security environment require that individuals all but have to give up their privacy, at least as far as law enforcement is concerned.

8.1 United States

In the US, the Bush administration has established the Office of Homeland Security in response to the events of September 11. Indeed, the Sydney Morning Herald's Good Weekend reported in June on the In-Q-Tel model of government agencies providing venture capital to invest in companies that are developing cutting edge technologies that might be useful for national intelligence.[26] The article also reported that the national security "killer app" will allow government agencies to access and share a wide

variety of personal information which is currently contained in different databases, from someone's shopping history to their parking tickets, and perhaps even their child support payment history.

When software applications are used by government to track, classify, profile and monitor citizens, they risk becoming technologies of state surveillance and discrimination rather than technologies of liberty.

8.2 New EU data protection directive

EU Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic environment (**New Directive**) was adopted on 12 July 2002.

The New Directive requires telecommunication companies and ISPs to retain traffic data such as e-mail for criminal investigation purposes or to safeguard national and public security. The proposal has been attacked by over 40 different civil liberties groups in Europe and the US who feel that the proposal would allow European governments to put ISPs and phone companies in the 'spy business'.

8.3 Australian anti-terrorism legislation

The Commonwealth government has recently passed five pieces of anti-terrorism legislation.[27]

The anti-terrorism legislation is designed to provide authorities with additional tools to combat terrorism and prosecute offenders. It does this by giving particular agencies additional powers to monitor the actions of individuals by collecting, using and disclosing personal and other information.

In April, the Privacy Commissioner made a submission to the Senate Legal and Constitutional Legislation Committee which stated that "the balance between the right to privacy and the right to feel secure has not been met in every instance"[28].

9 Conclusion

With the pervasive influence of technology into every day life, ranging from closed circuit television surveillance to DNA profiling, there is increasing evidence that these practices cannot be allowed to proliferate without a counterbalancing recognition of an individual's 'right' to privacy.

To conclude with the words of the Privacy Commissioner:

> "Striking the balance between the right to privacy and the right to feel safe and secure is not always an easy thing to do. Finding the balance, however, is a challenge that befalls the parliaments of all democracies and has done so throughout history."[29]

---

* With thanks to Duncan Giles (Special Counsel, Freehills) for his comments and assistance.

1 Available at http://www.privacy.gov.au/privacy_rights/npr.html
2 http://www.privacy.gov.au/news/media/02_12.html
3 John Cooper, 'Privacy: is greater cultural awareness required?', April 2002, http://www.findlaw.com.au/articles/default.asp?task=read&id=4018&site=CN
4 The Aulich report is not publicly available. Terry Aulich, (Director, Aulich), spoke generally about the report at the IT Security 2002 conference in April 2002. For a general article on the Aulich report and the conference, see Sandra Rossi, 'Big business rates low on privacy report', April 2002, http://www.computerworld.com.au/idg2.nsf/All/9CEF1EA68F8B4BDACA256BAA0078D186!OpenDocument&NavArea=&SelectedCategoryName=ros
5 ibid
6 James Riley, 'Private investigations', March 2002, http://www.itnews.com.au/story.cfm?ID=9224
7 http://www.privacy.gov.au/news/media/02_8.html
8 'Ridiculous law silences coaches', *Courier Mail*, 9 April 2002
9 http://www.privacy.gov.au/faqs/cf/q5.html
10 http://www.privacy.gov.au/news/media/02_5.html
11 Available at http://www.ica.com.au/privacy principles/privacycode.pdf
12 Available at http://www.clubsqld.com.au/privacy_code/PC_main.html
13 http://www.computerworld.com.au/IDG2.NSF/All/E8CF071F88677107CA256BE30025DBFD?OpenDocument
14 Available at http://www.privacy.gov.au/publications/mou03_02.pdf
15 http://www.privacy.gov.au/news/media/02_3.html
16 Dixon, T., "Preparing for new privacy legislation", Computers and Law, March 2001, p4
17 http://www.privacy.gov.au/publications/nppgl_01.pdf, p30
18 http://www.wired.com/news/privacy/0,1848,51461,00.html?tw=wn_ascii
19 http://www.theage.com.au/articles/2002/09/24/1032734153417.html
20 Property Law Act 1974 (Qld)
21 Property Law Act 1969 (WA)
22 Law of Property Act 2002 (NT)
23 Contracts (Rights of Third Parties) Act 1999
24 Contracts Privity Act (NZ) 1982
25 Available at http://www.iia.net.au/IIA_PrivacyCode(EUdraft).pdf
26 Good Weekend, Sydney Morning Herald, June 8-9, 2002
27 Security Legislation Amendment (Terrorism) Act 2002; Suppression of the Financing of Terrorism Act 2002; Criminal Code Amendment (Suppression of Terrorist Bombings) Act 2002; Border Security Legislation Amendment Act 2002; Telecommunications Interception Legislation Amendment Act 2002.
28 Available at http://www.privacy.gov.au/publications/secleg.pdf, p1
29 ibid