Australia: 2001 update

report by Nigel Waters

THE LAST YEAR has seen many developments in privacy regulation in Australia at both federal and state levels. In December 2000, the Privacy Amendment (Private Sector) Act passed through the Federal Parliament, and takes full effect in December 2001.

This Act has extended the Privacy Act 1988 to cover larger businesses in the private sector, subject to some major exemptions such as employee records, the media and political parties. Organisations are required to comply with ten National Privacy Principles (NPPs), based on the voluntary principles developed by the Privacy Commissioner through an extensive consultation process in 1997-98. The rights that individuals have had in relation to federal agencies since 1989 – to complain about breaches of the principles, and to access and correct data about themselves subject to exemptions – are extended to the private sector.

CODES OF PRACTICE FOR DISPUTE RESOLUTION

A novel feature of the new private sector regime is the provision for Codes of Practice which can not only replace the NPPs, (as long as the overall protection is not weakened) but can also introduce a sectoral Code Adjudicator as the first level of external dispute resolution. The government had intended this to be a complete substitute for the statutory complaint handling regime, but an amendment forced by the Senate made the decisions of Code Adjudicators subject to appeal to the Privacy Commissioner.

The federal Commissioner has issued three sets of draft guidelines to date this year on the operation of the new regime. These cover Code development and approval; interpretation of the NPPs, and the application of the law to the health sector. The first two in particular have proved controversial. The Code guidelines starkly demonstrate the high standards of both consultation and independence that will be required to gain approval of a Code that includes a Code Adjudicator. It is clear that establishing and maintaining such machinery will be costly. As a result, several industry sectors that were expected to submit a Code for approval are re-considering.

NPP GUIDELINES CRITICISED BY BUSINESS

The NPP Guidelines have been even more controversial. In them, the Commissioner has taken a position which favours individuals' interests over those of organizations much more than had been expected. His interpretation on such matters as the meaning of consent (how informed?, how free?); the need to specify a single primary purpose of collection, and the requirements for opt-in or opt-out for direct marketing have been strongly criticized by business groups, and in some cases do not appear to be well founded in law. Revised guidelines are expected by October.

The federal government has convened a consultative group to review existing Commonwealth privacy laws to consider whether there is a need for more specific protection of children's personal information. The group, which includes the Federal Privacy Commissioner, will consider a discussion paper on children's privacy prior to its release for public consultation to ensure that all relevant issues have been fully canvassed.

NEW SOUTH WALES

In July 2000, the New South Wales Privacy and Personal Information Protection Act 1998 came fully into force, with public sector agencies becoming liable for breaches of the twelve Information Protection Principles. Agencies were required under the Act to have lodged a Privacy Management Plan with the Privacy Commissioner. However, many agencies were late and the Commissioner has a backlog of Plans to consider. He has also been dealing with a larger than expected number of applications for Codes of Practice, which can lower (but not raise) the standards in the Principles.

The Codes deal with matters as trivial as allowing disclosures without consent where a person is being considered for an honour or award, to matters as significant as the regime for transfers to other jurisdictions. Critics have found disturbing the granting of so many 'waivers' to what was already a fairly weak law, with many exemptions.

The Commissioner's office is grossly under-resourced, with only the five staff of the previous Privacy Committee to administer a much wider law, and the Commissioner himself – Chris Puplick – is only part-time.

In June 2001, the NSW Attorney-General announced that the government would legislate to regulate surveillance generally in the workplace, pre-empting an expected recommendation of the State Law Reform Commission. The surveillance legislation will follow the model of the existing Workplace Video Surveillance Act 1997, which makes a

distinction between overt monitoring (requiring compliance with prescribed standards) and covert surveillance (allowed only with a judicial warrant).

VICTORIA

Victoria's Information Privacy Act was enacted in September 2000 and comes into full effect in September 2001. The Act requires State agencies to comply with Information Privacy Principles, which are, in fact, an earlier version of the Privacy Commissioner's NPPs. A Privacy Commissioner has been appointed – former journalist and consumer advocate Paul Chadwick – and he will be supported by about 12 staff. His jurisdiction is primarily the State public sector (excluding health) but some of his general functions allow him to comment on a wider range of privacy issues. A separate Health Records Act, passed early in 2001, establishes a customized set of principles for health information, to take effect in July 2002.

Despite Victoria having two new privacy laws, the newly re-established Victorian Law Reform Commission is to have privacy as one of its first references. In launching the Commission in April 2001, the Attorney-General asked that it "examine the coverage of privacy legislation for Victorians and to advise on priority areas for reform." The Commission issued a scoping paper in July, prior to formalizing terms of reference for the Inquiry.

The State Parliament's Scrutiny of Acts and Regulations Committee has issued a report on an Interim Privacy Code for Victorian Members of Parliament, pursuant to a Ministerial reference arising from the debate in December 2000 on the then Information Privacy Bill. The Bill as introduced applied to MPs, but they were exempted, by cross party agreement, on condition that a "voluntary" code of conduct be drawn up in 2001. The Committee has invited comments on the draft Code contained in its report.

OTHER AUSTRALIAN INITIATIVES

During the year several public sector initiatives have raised significant privacy issues.

Australian big business seeks to delay new private sector Data Protection Legislation?

by Eugene Oscapella

The online publication Australian IT reported on August 28th that "big business is flexing political muscle" to delay implementation of the Privacy Amendment (Private Sector) Act 2000, which will regulate the handling of personal information by private sector organisations. The Act is due to take effect on December 21st 2001. However small businesses, except health services, covered by the new provisions have an additional twelve months until December 21st 2002.

Australian Prime Minister, John Howard, was reported to be concerned by the strength of feeling expressed by retailers about the laws, and promised to raise the matter with the Attorney-General.

Australian Retailers Association president, Hans Mueller, urged Mr Howard to delay the legislation for a year. The Association's chief executive, Phil Naylor, said that it supported the legislation but because the guidelines were not finalised, the Government should consider pushing back the operative date of the Act.

Under the new law, consumers will have access to personal information held by businesses, the right to correct errors, and the right to insist on removal from direct-mail lists.

For further information see www://australianit.news.com.au/common/storyPage/0,3811,2699839%5E442,00.html

Forensic evidence and DNA

A new system for collecting, storing and using DNA samples for law enforcement came into effect. Complementary federal and state laws dealing with forensic evidence have been passed and a new federal agency – CRIMTRAC – established. Samples are now being collected not only from suspects in new crimes, but also compulsorily from prisoners to match against crime scene evidence for unsolved crimes. The legislation also provides for samples to be taken from volunteers in the course of major crime investigations. Some privacy safeguards have been put in place, but it remains to be seen if they are effective.

Cybercrime

Early in 2001, state and federal governments issued a report on a Model Criminal Code Damage and Computer Offences. NSW has already enacted its version of the law without any opportunity for debate. At least, the equivalent federal Cybercrime Bill 2001 is under consideration by a Senate Committee. The federal Bill has two main components changes to the definitions of computer offences; and new investigatory powers for the federal police and other law enforcement agencies.

Both parts have been strongly criticized – not only by privacy and civil liberties groups but also by the Information Technology industry. Technologists say that the new computer offences are so broadly drawn that they will inadvertently criminalise many innocuous and even essential activities. Concerns have also been expressed about the justification for and breadth of investigative powers.

Pharmaceuticals

In May 2001, the federal health department put out a draft Bill to implement a Better Medication Management System (BMMS). This system would provide for a centralized national database of prescriptions and dispensing of pharmaceuticals. Although the draft legislation was based on a voluntary opt-in model (both for patients and providers), it was widely criticized, not least on privacy grounds. It is understood that the Health Department is reconsidering its approach. In the meantime, all jurisdictions are discussing various proposals for electronic health records, and privacy issues are at least recognized as highly significant.

Encryption

The federal government has also been developing a framework for the use of public key infrastructure (PKI) in government. It is also being forced, reluctantly, to recognize the implications for wider use in all sectors. As part of this recognition, the National Office for the Information Economy (NOIE) has funded a project which has resulted in draft PKI privacy guidelines from the federal Privacy Commissioner. These guidelines acknowledge the significance of such matters as an individual's ability to have more than one digital certificate, providing for attribute certificates which do not require identification, and access to certificate revocation lists as a form of transaction monitoring.

Nigel Waters is director of Pacific Privacy Partners in Australia.
Tel: +61 2 4981 0828
E-Mail: nigelwaters@primus.com.au