HAVE PRIVACY LAWS DELIVERED?

By Nigel Waters

In the last two decades, Australia has acquired a complex and confusing patchwork of privacy laws. This article assesses these laws and finds them wanting. Flawed principles, weak enforcement mechanisms and lack of commitment from government and business combine to leave Australians with only limited privacy protection.

Photo © Lana Vshivkoff

It is now 18 years since the federal *Privacy Act* 1988 introduced the first set of statutory information privacy principles in Australia. The Australian Law Reform Commission (ALRC) is now reviewing privacy laws.[1] How well have the laws performed?

AUSTRALIAN PRIVACY LAWS

The *Privacy Act* originally applied to Commonwealth and ACT government agencies, requiring them to comply with a set of privacy principles set out in the Act, and to the use of tax file numbers, with specific guidelines included in the Act but subsequently revised by the Privacy Commissioner. In 1990, the Act was extended to cover consumer credit reporting and, in 2000, to most large private-sector businesses, but with major exemptions for employee records, small businesses, political parties and the media.

Privacy principles were legislated for the public sector in NSW (1998), Victoria (2000), the Northern Territory (2002) and Tasmania (2005). The remaining states have adopted versions of the principles for their public sector agencies but only as administrative guidelines, with no active monitoring and enforcement mechanism equivalent to the federal, NSW, Victorian or NT Privacy or Information Commissioners. The ACT, NSW and Victoria also have specific health privacy laws covering both private and public sectors, while most states have some form of surveillance law, currently being updated or reviewed.[2]

PRIVACY PRINCIPLES

The principles found in Australian privacy laws share a common origin – the Organisation for Economic Co-operation and Development principles of 1980, subsequently adopted in Europe, Canada and elsewhere, including New Zealand in 1993. All versions of the principles cover the same ground by imposing obligations on 'data-users' throughout the lifecycle of personal-information handling – from collection, through to storage, use and disclosure to disposal. They require notice to individuals, transparency about information-handling practices, appropriate security, quality standards, and they confer a right of access and correction (which, in the public sector, re-inforces existing rights under freedom of information laws).

While superficially comprehensive, most privacy principles are handicapped by requiring only that data-users take 'reasonable steps' in order to comply. This leaves considerable scope for discretion by agencies and organisations as to how seriously to take them. The effectiveness of the principles relies, ultimately, on how strictly they are interpreted by regulators, tribunals and courts. In NSW, there are now around 100 privacy decisions by the Administrative Decisions Tribunal, including some significant awards of compensation, as well as some major decisions limiting the law. Some early decisions by the Victorian Civil and Administrative Tribunal are also significant.[3] In contrast, the Federal Privacy Commissioner has made only eight formal complaint determinations in 17 years and seems to be averse to committing to a firm interpretation of the principles.[4]

Overall, the privacy protection offered to individuals is limited, fragmented, and overly complex.

Another feature of privacy principles is that the limits on using and disclosing information – which on their face are the most powerful protections – are, in reality, fatally compromised by the range of exceptions. While these principles are often 'sold' as giving individuals control over how information about them is used, exceptions for secondary uses give data-users considerable discretion to do things without individuals' consent. Exceptions for uses 'authorised or required by law' mean that many unexpected and unwelcome uses are already lawful, and it is open to governments to change the boundaries at any time. The supposed requirement for consent is therefore largely meaningless.

MAJOR FAILINGS

Overall, the privacy protection offered to individuals is limited, fragmented, and overly complex. Its prospects of ever being sufficiently clearly and widely understood – such that businesses and government agencies will adopt the 'culture of privacy' being promoted by Privacy Commissioners, or that individuals will be able to effectively exercise their rights – are limited. Community attitudes research commissioned and published by the Office of the Federal Privacy Commissioner (OPC) in 2004[5] revealed low levels of awareness, understanding and satisfaction, and demonstrated that the legal privacy protection regime does not currently meet community expectations.

At the federal level, the *Privacy Act* runs the serious risk of legitimising intrusive practices and giving individuals a false and misleading sense of protection. Businesses and government are now able to make a general claim that privacy is protected by the Act, when the reality is that there are so many exemptions and exceptions that this is simply not true in many settings and circumstances.

Nor are the penalties under the *Privacy Act* sufficient to act as a significant deterrent. While the Commissioner can theoretically award unlimited compensation, the maximum negotiated to date is $25,000. The vast majority of conciliated complaints have resulted in apologies, agreement to change practices and, in a small number of cases, token payments of a few hundred dollars. It is interesting to compare the *Privacy Act* regime with the recent telecommunications privacy legislation: the *Spam Act* 2003 and the *Do-Not Call Register Act* 2006[6] include significant civil penalties, criminal offences and strong enforcement powers for the regulator – the Australian Communications and Media Authority (ACMA). Only recently, a West Australian spammer was fined $5.5 million.[7]

>>

> Recent legislation has expressly authorised privacy intrusions that would otherwise be unlawful.

The weakness of the statutory framework for privacy protection both for the private sector and for government is compounded by the wholly inadequate resources devoted to its administration, promotion and enforcement. Both absolutely and by comparison with other regulatory bodies, the OPC is grossly underfunded, resulting in such major deficiencies as unacceptable backlogs of complaints and effective cancellation of a discretionary audit program (in those jurisdictions where that applies). A significant budget supplement in 2006 is unlikely to make more than a marginal impact.

Under-funding of the OPC, and the weakness of the regulatory scheme, also contribute to a widespread perception in the business community that the Act is a 'paper tiger', and that government does not take the enforcement of privacy rights seriously, other than at the most superficial level. Because of the low probability that breaches will be detected, and the minor consequences if they are, private sector businesses are likely to give a low priority to privacy compliance.

Larger businesses and their industry associations predictably pay lip-service to their compliance obligations and claim to support the objectives of the Act. This is largely superficial and does not typically translate into significant resources for training, inclusion of privacy considerations in major corporate decisions, or internal enforcement.

Even in the public sector, there is evidence that privacy laws are not being taken seriously. Major Commonwealth government agencies, such as Centrelink and the ATO, which should – after 17 years of privacy laws – have a deeply embedded culture of respect for privacy, still find themselves having to discipline hundreds of staff for unauthorised uses of personal information.[8] A wave of anti-terrorism, law enforcement and border-control legislation in recent years has expressly authorised privacy intrusions that would otherwise have been unlawful under the *Privacy Act*. It seems as though agencies need only mention some wider public interest to have any constraints of privacy law removed.

At the state level, privacy laws seem to be treated with even less respect. The NSW government has effectively torn up a key principle of its own health privacy law to allow electronic health records to be shared without consent,[9] has removed prisoners' privacy rights,[10] and given the administration of the new photo identity cards for non-drivers to the Roads and Traffic Authority (ensuring that a central database of photographs of almost the entire state population is available for a wide range of law enforcement and other purposes).[11] The NSW government has also failed to appoint a permanent Privacy Commissioner for more than three years, and has slashed the resources of Privacy NSW. While the first Victorian Commissioner was given reasonable resources for his five-year term, this expired in July 2006 and a permanent replacement has yet to be appointed. The future of the Victorian office as an independent watchdog is not assured.

The latest vogue in privacy protection is the use of privacy impact assessments (PIAs) for new initiatives. When done well and published, PIAs can make a significant contribution, but too many have been suppressed,[12] presumably because they contained unwelcome analysis and recommendations. Where they have been published, they have largely been ignored.[13] As with privacy laws themselves, there is a serious risk that PIAs allow governments to appear to take privacy seriously, while proceeding largely unchecked with highly intrusive new programs.

CONCLUSION

Overall, the privacy laws introduced in Australia since 1988 have not lived up to their promises. The ALRC has a major opportunity, with its two-year privacy inquiry, to put privacy law back on track. Its initial issues paper is encouraging in its breadth and apparent interest in the fundamental rationale and foundations of privacy in human rights law.[14] Whether this interest survives the inevitable pressure from government and business remains to be seen. ■

Notes: **1** See http://www.alrc.gov.au/inquiries/current/privacy/about.html (26 November 2006). **2** For the best index of privacy laws, see http://www.privacy.vic.gov.au/dir100/priweb.nsf/content/2A43C5DD5A412761CA256FA400110051?OpenDocument (26 November 2006). **3** See http://www.worldlii.org/int/special/privacy/virtual_db/cases/ (26 November 2006) for selected privacy cases from all Australian jurisdictions. **4** An Australian Research Council-funded comparative research project at the University of New South Wales is seeking to draw common threads out of the guidance and decisions from a range of jurisdictions: see http://www.cyberlawcentre.org/ipp/ (26 November 2006). **5** See http://www.privacy.gov.au/publications/rcommunity/index.html (26 November 2006). **6** Also replicated in the Telecommunications Legislation Amendment (Integrated Public Number Database) Bill 2006. **7** *Australian Communications and Media Authority v Clarity1 Pty Ltd* [2006] FCA 1399. **8** See http://www.abc.net.au/news/newsitems/200608/s1721505.htm and http://www.news.com.au/sundaymail/story/0,,20696707-953,00.html (both 26 November 2006). **9** Regulations for the HealtheLink trials have provided for an 'opt-out' approach, reversing the 'opt-in' requirement of Health Privacy Principle 15 in the *Health Records and Information Privacy Act* 2002 (NSW). **10** *Privacy and Personal Information Protection Amendment (Prisoners) Act* 2002 (NSW). **11** *Photo Card Act* 2005 (NSW). **12** Most notably the PIA on the federal government's so-called 'access card'. For details of the lack of transparency, see http://www.privacy.org.au/Campaigns/ID_cards/HSAC.html (26 November 2006). **13** Such as the PIA on the Anti-money Laundering and Counter-terrorism Financing Bill 2006 – 66 of 96 recommendations were rejected outright and many others were only partially accepted. See http://www.ag.gov.au/www/agd/agd.nsf/Page/Anti-money_laundering (26 November 2006). **14** slssues Paper 31, October 2006, http://www.austlii.edu.au/au/other/alrc/publications/issues/31/.

Nigel Waters *is the Principal of Pacific Privacy Consulting, and Policy Co-ordinator of the Australian Privacy Foundation.*
PHONE *(02) 4981 0828* **EMAIL** *nigelwaters@iprimus.com.au*
WEBSITE *http://home.iprimus.com.au/nigelwaters/*