Amendment Bill 2007, p 8.

6 For example, the digital transmission platform adopted in South Korea (Digital Multimedia Broadcasting) carries a combination of digital TV, digital radio and data channels.

7 BSA ss 8AC(3)(a).

8 BSA ss 8AC(3)(b).

9 http://www.acma.gov.au/WEB/STANDARD/pc=PC_310504.

10 BSA ss 8AA and 8AD(3).

11 These funding commitments are in the Federal *Budget 2007-08* at http://www.budget.gov.au/2007-08/bp2/html/expense-05.htm.

12 The Government's 2003 policy announcement (see note 2) states that the Government might, in the future, provide capped financial assistance for commercial radio broadcasters in regional areas.

13 BSA ss 35C and 35D(2).

14 Explanatory Memorandum accompanying the *Broadcasting Legislation Amendment (Digital Radio) Bill 2007* and the *Radio Licence Fees Amendment Bill 2007* p. 39.

15 http://www.wohnort.demon.co.uk/DAB/index.html.

16 CRA is the industry body for the commercial radio sector and its trial is being conducted as a joint venture with commercial radio stations and the ABC and SBS. For more on its trials, see http://www.commercialradio.com.au.

17 http://en.wikipedia.org/wiki/Digital_Audio_Broadcasting.

18 CRA, "Australia to use DAB+ for Digital Radio Rollout", 14 March 2007 at http://www.digitalradioaustralia.com.au/index.cfm?page_id=1001&display_news_id_1129=1002. More information on DAB+ can be found on the website of the technical standard setting body WorldDMB at http://www.worlddab.org.

19 Explanatory Memorandum accompanying the *Broadcasting Legislation Amendment (Digital Radio) Bill 2007* and the *Radio Licence Fees Amendment Bill 2007* p 6. DRM is currently being trialled by Broadcast Australia in Canberra. DRM does not have all the features of DAB and is said to be a narrowband service with the audio quality of a mono FM radio service.

20 BSA s 215A.

21 Radcomms Act s 5.

22 Radcomms Act s 118NR.

23 Radcomms Act s 118NS.

24 Radcomms Act s 5.

25 Radcomms Act .s 118NT.

26 Radcomms Act s 118NV.

27 Radcomms Act ss 102F and 118NU.

28 Radcomms Act ss 102C(2) and 102D(2).

29 Radcomms Act ss 102C(3) and 102D(3).

30 Radcomms Act ss 102C(4) and 102D(4).

31 Radcomms Act s 118ND.

32 Radcomms Act s 118NL and 118NM.

33 Radcomms Act ss 118NZ and 118P.

34 Radcomms Act ss 118NF(4).

35 Radcomms Act ss 118NF(5).

36 Radcomms Act s 118PE.

37 Radcomms Act s 118H.

38 Radcomms Act s 118L.

39 http://www.accc.gov.au/content/index.phtml/itemId/798925.

40 Above n 18.

41 BSA ss 43D(3) and 43D(4).

42 See the definition of 'digital program enhancement content' BSA. s 6(1).

43 http://www.commercialradio.com.au/index.cfm?page_id=1001&display_news_id_2400=1039.

44 Explanatory Memorandum accompanying the *Broadcasting Legislation Amendment (Digital Radio) Bill 2007* and the *Radio Licence Fees Amendment Bill 2007*, pp 38-39.

45 Explanatory Memorandum accompanying the *Broadcasting Legislation Amendment (Digital Radio) Bill 2007* and the *Radio Licence Fees Amendment Bill 2007* p. 56.

46 BSA s 54B.

47 BSA s 215B.

48 BSA s 13B.

Radical Privacy Law Reforms Proposed

Dr Gordon Hughes and Tim Brookes discuss the Australian Law Reform Commissions recent discussion paper on Australian Privacy Law.

Introduction

On 12 September 2007, the Australian Law Reform Commission (**ALRC**) released a 2,000 page discussion paper entitled *Review of Australian Privacy Law*. The discussion paper sets out the ALRC's preliminary views on how Australia's complex privacy laws could be revamped and calls for comments from interested parties by 7 December 2007. A final report to the Attorney General is due by 31 March 2008.

Traditionally, it has been accepted that there is no right to privacy at common law in Australia although some recent decisions have introduced an element of uncertainty. There is, however, extensive privacy legislation. The legislative framework is essentially embodied in the *Privacy Act 1988* (Cth) (**Privacy Act**), complemented by the *Spam Act 2003* (Cth), the *Do Not Call Register Act 2006* (Cth), segments of the *Telecommunications Act 1997* (Cth) and *Telecommunications (Interception and Access) Act 1979* (Cth) and a range of State and Territorial laws, regulations and policies.

The Privacy Act has been amended on numerous occasions, and imposes separate regulatory regimes on the handling of personal information held by Commonwealth government agencies and the private sector, along with specific rules regulating the handling of tax file numbers and certain credit information.

Unquestionably, the existing system has become cumbersome and confusing.

Consolidation Of Privacy Principles

Personal information held in the Commonwealth public sector is regulated by the Information Privacy Principles set out in Section 14 of the Privacy Act. Information held in the private sector is regulated by the National Privacy Principles set out in schedule 3 of the Act. There are some inconsistencies between the two sets of regulations and, in the case of Commonwealth outsourcing to the private sector, a service provider may have a statutory obligation to comply with the National Privacy Principles and a contractual obligation to comply with the Information Privacy Principles. The ALRC recommends that these two sets of privacy principles be consolidated into new 'Unified Privacy Principles'. The rationalisation of the currently inconsistent principles would result, amongst other things, in a limited right for individuals to deal with government agencies anonymously, more robust rules dealing with the handling of sensitive information in the public sector and constraints on public sector agencies transmitting personal data overseas. Furthermore, the ALRC urges clarification as to what amounts to 'consent', clearer rules governing the handling of third party information, more flexibility to disclose information in urgent situations, greater restraints on the collection of irrelevant information and a more efficient process to enable the correction of inaccurate information.

Embracing New Technologies

The ALRC has recognised the need for the Privacy Act to be adaptable so as to address privacy issues posed by new technologies. It notes, in particular, challenges presented by relatively recent technology such as spyware, cookies, radio frequency identification technology and biometric information technology. To guard against any legislative reform becoming prematurely outdated, the ALRC stresses the importance of the legislation remaining technologically neutral. The report also encourages the adoption of – and public education about – privacy enhancing technologies. The ALRC further recommends that email and IP addresses be unambiguously protected by the legislation as 'personal information', and the report raises the possibility of the introduction of a 'take down notice' scheme requiring website operators to remove information which constitutes an invasion of an individual's privacy.

Removal of Exemptions

Privacy obligations currently imposed by the *Privacy Act* do not apply to organisations with an annual turnover of less than $3 million, political parties or acts in the course of journalism of media organisations which have committed to privacy standards. In addition, employee records are exempt from the existing scheme. The ALRC proposes that exemptions applicable to small business, political parties and employee records should be removed. It is proposed, on the other hand, that the media exemption be retained on the basis that it is necessary to balance privacy protection on the one hand and the free-flow of information to the public on the other. The media exemption will be restricted, however, to news, current affairs and documentary material. In addition, the ALRC proposes that standards 'adequately' deal with privacy in a media context and proposes various measures to achieve this. It also proposes that the new cause of action discussed below would apply to acts in the course of journalism as well as to other activities. That is, the media exemption would not apply in respect of the proposed cause of action.

Telecommunications and Marketing

The ALRC proposes an amendment to the *Telecommunications Act 1997* (Cth) to prohibit carriers charging for unlisted telephone numbers.

In relation to spam and telemarketing, the report queries whether regulation imposed by the *Spam Act 2003* (Cth), currently restricted to telephone numbers and email addresses, should be expanded to cover facsimile and Bluetooth messages, and whether government agencies and political parties should be required to incorporate an unsubscribe facility into spam which is otherwise permitted under exemptions set out in schedule 1 of the Act. The ALRC further foreshadows the possible extension of the *Do Not Call Register Act 2007* (Cth), which currently regulates telemarketing calls, to incorporate the regulation of Voice Over Internet Protocol (**VOIP**) numbers and it queries whether the exemption for political parties and politicians set out in Schedule 1 to the Act should be removed.

The report further foreshadows the introduction of a special privacy principle to deal with direct marketing. The principle would apply regardless of the purpose for which information was collected and the report foreshadows the application of direct marketing restrictions on public sector agencies.

Regulation of Health Records

Privacy obligations in respect of health information are implemented inconsistently throughout the country. The Privacy Act provides a higher level of protection to 'sensitive information', which includes 'health information', whilst other States and Territories (apart from Western Australia and South Australia) have adopted a range of legislative and regulatory controls. The ALRC has proposed health privacy regulations to operate in conjunction with the proposed new Unified Privacy Principles, and State and Territory health services would be 'encouraged' to develop health regulations consistent with the new Commonwealth regulations. New laws would facilitate the collection by healthcare providers of information on third parties without their consent where this was relevant and necessary for treatment, and patient access to healthcare records would be facilitated in certain circumstances. The ALRC also foreshadow the possible introduction of a shared electronic health record system which in turn would require the regulation of unique healthcare identifiers (discussed further below).

Credit Reporting and Identity Theft

The report acknowledges the benefit inherent in credit providers having access to a greater range of information whilst at the same time recognising that the collation of an expanded range of information potentially increases privacy risks. The ALRC suggests that an expanded range of information be permitted but that it be subject to review after 5 years of operation. It is further proposed that credit reporting agencies be subjected to a greater obligation to monitor the accuracy of information on individuals supplied by credit providers and that they should establish controls to ensure that information used or disclosed is accurate, complete, up-to-date and relevant. A credit provider wishing to provide information on defaults to a credit reporting agency would have to be a member of an external dispute resolution scheme, and the report proposes a time limit of 30 days in which a credit provider must respond to the notification by a consumer that a default listing is disputed. The collection of credit information from individuals known to be under the age of 18 would be prohibited, and individuals would be entitled to report that they had been the victim of identity theft so as to ensure that such information would be available to any potential credit provider.

Regulation of Identifiers

The ALRC urges the introduction of greater controls over the use of personal 'identifiers', such as customer numbers. In this regard, it recommends an expanded definition of 'identifier' to include biometric information and symbols as well as numbers, greater regulation of identifiers used by public sector agencies, expanded powers for the Privacy Commissioner in determining what constitutes an 'identifier' and the regulation of identifiers issued by State government agencies (such as driver's licence numbers). One specific form of identifier referred to in the report is a possible unique healthcare identifier which would be introduced with the advent of a shared electronic health records system. It would be necessary to legislate specifically in relation to the permitted and prohibited uses of unique healthcare identifiers and information in electronic health records and to introduce safeguards in relation to unique healthcare identifiers, such as a guarantee that it would not be necessary to produce such an identifier in order to obtain healthcare services.

Transborder Data Flows

Existing restrictions on transborder data flows apply only to private sector organisations. The ALRC proposes that requirements protecting information sent overseas should now be extended to public sector agencies. At present, it is possible for a private sector organisation to transmit personal information overseas, if, inter alia, the organisation believes that the body receiving that data is subject to a law which imposes similar privacy requirements about the handling of information. The ALRC proposes greater guidance on what amounts to 'adequate overseas privacy laws' for these purposes. The report further proposes that the ability of an organisation to transfer personal information overseas by relying upon the existence of other conditions, such as the fulfilment of contractual obligations or the impracticality of obtaining consent of the individual, be more closely regulated.

Statutory Cause of Action

Until 2001, a decision of the High Court of Australia in 1937 was commonly understood to mean that a general right of privacy did not exist at common law. In 2001, the High Court found that the 1937 decision had a narrower significance and that a right of privacy might well exist. The majority of the Court canvassed the possibility of a tort of privacy like one that exists in the United States. Gleeson CJ found in accordance with United Kingdom case law that breach of confidence principles protect private information in particular circumstances. The 2001 High Court decision has led to subsequent awards of damages for breach of privacy in both the Queensland District Court and the Victorian County Court. There have also been findings by other Courts that no such cause of action yet exists. Thus, the common law position in Australia is highly uncertain. The ALRC has proposed a statutory cause of action for invasion of privacy in circumstances which include where there has been interference with an individual's home or family life, the individual has been subject to unauthorised surveillance or sensitive facts about an individual's private life have been disclosed. The cause of action would apply where there was a reasonable expectation of privacy and where the infringement was serious enough to cause 'substantial offence to an ordinary person'.

Gordon Hughes and Tim Brookes are Partners at Blake Dawson. Gordon Hughes is based in Melbourne and Tim Brookes in Sydney.