Telecommunications privacy at the crossroads

***Tim Dixon** summarises the Centre's discussion paper on privacy issues relevant to the telecommunications industry*

After five years in which telecommunications issues have gradually assumed a higher profile in the privacy debate, Australia is about to establish the legislative framework which is likely to govern the telecommunications industry and establish privacy protection well into the next decade.

Technological developments are making privacy an increasingly important issue in telecommunications regulation. Calling number display technology, telemarketing, encryption and digital authentication raise significant privacy issues. The convergence of communications and information technologies and the increased capacities of information processing and use have heightened concerns about the inadequacy of Australia's current privacy protection regime. The current mix of telecommunications and privacy laws provides very little protection for the privacy of communications or for the privacy of telecommunications-related personal information. The full deregulation of the telecommunications industry raises additional privacy concerns, with a likely increase in the use of personal information.

Late last year, federal Attorney-General Daryl Williams announced his government's plan to introduce new privacy legislation covering both the public and private sectors. The announcement was accompanied by a discussion paper outlining the Government's proposed framework for privacy legislation.

IPPs

The government proposes that the new privacy legislation will be based the Information Privacy Principles, mostly unchanged from the present Privacy Act 1988. The legislation will provide for the development of codes of practice 'in relation to specified information, activities, organisations, industries or professions...to elaborate on the IPPs...to provide concrete details on issues of relevance to a part of the private sector...[or] to modify the IPPs'.

The proposal for regulation of the private sector through codes and the IPPs is the most controversial feature of the government's proposal. Codes would be issued by the Privacy Commissioner on his or her own initiative, or on the application of any person. Codes do not need to be comprehensive, and they can even differ from the IPPs on only one issue. They may strengthen or weaken protections in the IPPs. The normal process for developing a code will involve public notification, development of a draft code, consideration of written submissions, and the release of the finalised code. An industry group might itself develop the code and then submit it to the Commissioner for approval. Breaches of a code, once enacted, would attract the same consequences as a breach of the IPPs.

Access to information

The legislation will also give individuals a limited right to access information about them held by a private or public sector organisation. This right is subject to a range of exemptions. Restrictions will be placed on the transborder export of personal information, requiring adequate safeguards to ensure that the privacy of individuals affected will be protected. Organisations will be made responsible to appoint an identifiable privacy officer to whom outside inquiries relating to privacy protection will be directed.

Media

As with the New Zealand legislation, the media is acknowledged as a special case because of the need to balance the public interest in freedom of expression with privacy protection. The paper promises that 'separate consideration' should be given to privacy issues relating to news media, without indicating how this may be done.

The Centre's submission

The Communications Law Centre's submission to the Attorney-General's Department advocates strengthening the privacy principles which will form the foundation of the new privacy legislation. These changes would address the major weaknesses of legislation, which mainly seeks to apply the Privacy Act 1988 to the telecommunications sector. The IPPs, based on 1981 OECD Guidelines, reflect thinking on the major privacy issues from twenty years ago. The proposed changes are largely based

on the principles contained in the Australian Privacy Charter.

Principle 1 – Justification: Most privacy and data protection legislation is flawed by the fact that it only addresses privacy issues raised by new technologies and systems in their final stages of implementation. Privacy legislation does not address the threshold question of whether there is adequate justification in the first instance for the use of a new technology which may compromise personal privacy. If privacy legislation only regulates information practices, its effect may be to legitimise systematic privacy invasion by failing to stop new technologies and systems which represent an unacceptable invasion of personal privacy.

The Privacy Charter proposes that any new system, technology or practice which may affect personal privacy should initially be justified as being in the public interest. This could be implemented systematically through conducting privacy impact assessments, 'a process whereby a conscious and systematic effort is made to assess...any actual or potential effects that [an] activity or proposal may have on individual privacy and the ways in which any adverse effects may be mitigated'. Based around the concept of the environmental impact assessment, an effective PIA would involve public consultation, the appropriate use of expertise, and independence. The concept of the PIA is receiving growing international support. It allows a community to consider the implications of privacy implications of new technologies in advance rather than retrospectively.

Principles 6-9 – Freedom from surveillance, privacy of communications, private space and physical privacy: The Charter is based on a belief that privacy principles should go beyond information privacy. The inclusion of principles recognising the rights of individuals to freedom from surveillance and privacy of communications would clearly bring within the ambit of the Privacy Commissioner issues such as the use of listening devices on telephone lines and video surveillance (including surveillance of future videophone services), and interception of email.

Principle 10 – Anonymous Transactions: The right to anonymity has emerged as a crucial issue during the debate over the introduction of smart card technologies. The principle states that people should only be required to identify themselves in transactions when there is a substantial public interest reasons why an individual should be identified. This principle establishes an individual's right to anonymity in communications such as making a telephone call or sending an email message. The right to anonymity strengthens the protection of free speech, although it may of course also widen the scope for defamatory comments and 'hate speech'. Exceptions to this principle would include transactions requiring an ongoing relationship between an individual and an organisation and which involve a significant level of risk, such as the provision of credit, or air travel.

Principle 17 – Public Registers: Public registers such as electoral rolls, births and deaths records, and land and titles records, contain a limited range of personal information. The Privacy Charter Council concluded that, given technological developments, there is a strong justification for controls over access to public registers, given that individuals often do not consent to the collection of personal information for public registers, but are legally required to provide it.

Principle 18 – No Disadvantage: This principle establishes that people should not be disadvantaged by asserting their right to privacy. Experience in the United States has shown that organisations sometimes establish information collection practices which are described as 'voluntary' but which financially disadvantage individuals who do not identify themselves or provide personal information. Privacy would thus come at a premium price, undermining its status as a fundamental right. The Charter states that the provision of reasonable facilities for the exercise of privacy should be a normal operating cost for business.

Media privacy: While the Discussion Paper notes that there are special issues associated with privacy protection and the media, it does not outline options for implementing privacy protection in the media. A number of self-regulatory codes in the media industry provide guidelines for protecting the privacy of individuals, and complaints may be lodged with regulatory agencies such as the Australian Broadcasting Authority.

While existing codes provide general recognition of the importance of privacy protection, they are too brief to provide significant guidance to journalists in striking an ethical balance between privacy interests and the journalist's task of disclosure. Although there are persuasive arguments for why the media should not be included in the scope of general privacy protection, there is nevertheless a need for improving the self-regulatory framework of privacy protection in the media. The interaction of privacy principles with media responsibilities needs to be reviewed, and detailed consideration should be given to the most appropriate framework which may strike a balance between privacy and other interests.❑

This article is based on the Communications Law Centre's research paper on Telecommunications Privacy, written by Tim Dixon (See Policy File)., Director, Australian Privacy Foundation