Personal and Private

Natasha Stott Despoja

The conservative agenda shifts away from privacy regulation in the telecommunications industry.

Natasha Stott Despoja is an Australian Democrats Senator for South Australia.

The new *Telecommunications Act 1997* (the Act) creates a privacy blackhole that should have been filled by the Coalition's pre-election commitment to a comprehensive public and private sector privacy scheme. This Act was passed with the expectation that comprehensive privacy laws would be extended to the private sector. The Prime Minister's decision to abandon private sector privacy legislation will adversely affect the interests of all Australia's telecommunications consumers. Instead of the promised legislative protection, consumers' privacy will be reliant on the corporate citizenship of the telecommunications industry.

Privacy protection needs to extend to the collection, storage, security, access, correction, use, destruction and disclosure of *all* personal information. The present legislative scheme set out in the *Privacy Act 1988* addresses the collection, storage, use and disclosure of personal information held by the Commonwealth Government. This scheme also extends to tax file numbers, credit reporting and in a limited way to certain telecommunications suppliers and operators. Other than these limited situations the *Privacy Act* does not extend to the private sector. The common law provides limited protection for a range of special relationships, such as that between a bank and its customers.

Consumer privacy concerns about telecommunications are becoming more focused. The telecommunications industry is leading technological changes where personal information now has value, is easily collected and stored and may readily be processed. It is arguable that their businesses depend on information protection to ensure their market share and to satisfy consumers that their personal information is safe. Collecting personal information and then processing that data has significant benefits for business. Take this example: 'In the retail trade ...computers have matched things like age, sex and credit card spending habits and discovered that on Friday nights, an extraordinary number of 30-year-old men develop an apparently compelling desire for two oddly juxtaposed items. They stop into supermarkets on the way home from work and pick up nappies and beer. That's lead to rapid rearrangement of shelves'.[1] Here information in the form of age, sex and credit card spending habits have been applied for commercial purposes. This is personal information and this personal information has commercial value which should be protected. The same concerns apply to the collection of personal information and its use by the telecommunications industry for calling number displays, telemarketing, reverse directory products, surveillance, unique identifiers, data matching, etc. These are valid consumer concerns and there should be adequate protections for consumer's personal information.

Government backflip on privacy

At the last election, the Coalition stated that the 'Coalition regards personal privacy as a cherished right in a free society'[2] and that the

Government would 'work with industry and the States to provide a co-regulatory approach to privacy within the private sector in Australia, comparable with best international practice'.[3] This commitment seemed to be in place when the Attorney-General launched a Discussion Paper[4] on 12 September 1996 saying 'Privacy protection will be enhanced for all Australians with the extension of the *Privacy Act* to the private sector ... I intend to be in a position to develop legislation for introduction next year'.[5]

The Discussion Paper released by the Attorney-General set out a scheme based on the existing Information Privacy Principles in the *Privacy Act* and met many of the concerns of consumers. It added Codes of Practice and a range of additional provisions which addressed the particular concerns of the private sector. In essence this was a proposal for industry codes of practice supervised by the Privacy Commissioner and subject to statutory backing — a co-regulatory approach. This scheme is consistent with the schemes adopted by New Zealand, Hong Kong, Taiwan and the European Union.

This proposed scheme would have applied to the telecommunications industry through amendments to the *Privacy Act* and codes of practice specific to the needs of the industry. The industry specific Codes of Practice would have been issued by the Privacy Commissioner and subject to the *Privacy Act* as if they were Information Privacy Principles and subject to the same complaint, investigation and enforcement powers.[6] The Privacy Commissioner would have had a central role in overseeing privacy in the telecommunications industry.

Then on 21 March 1997 the Prime Minister did a 'backflip'. He stated: 'I took the opportunity of today's Premiers Conference to raise the Commonwealth's concern's regarding proposals to implement a privacy regime for the private sector ... The Commonwealth will not be implementing privacy legislation for the private sector'.[7]

Without the extension of the *Privacy Act* to the private sector the limited privacy protections set out in the Act will have to be relied on. These provisions are unlikely to be adequate or compare favourably with the Coalition's pre-election commitment and Discussion Paper proposal.

Privacy regulation in the Telecommunications Act 1997

The *Telecommunications Act* sets out the means for regulating the telecommunications industry in Australia, including a scheme for regulating privacy through *industry codes* and *industry standards* among other matters (ss.112 to 135). The Australian Communications Authority (the ACA) will oversee this regulation, including any privacy scheme the telecommunications industry adopts.

Section 113 of the Act provides, in part:

> (1) This section sets out examples of matters that may be dealt with by industry codes and industry standards ...
>
> (3) The examples are as follows ...
>
> (f) privacy and, in particular:
>
> (i) the protection of personal information; and
>
> (ii) the intrusive use of telecommunications by carriers or service providers; and
>
> (iii) the monitoring or recording of communications; and
>
> (iv) calling number display; and
>
> (v) the provision of directory products and services ...

Where the industry develops an industry code it may be registered by the ACA after certain criteria have been satisfied (s.117). Alternatively, the ACA *may* request an industry code (s.118) or where no body or association represents a section of the telecommunications industry the ACA may request, by notice in the Gazette, that if such a body or association came into existence then a request would most likely be made (s.119). Where a registered industry code is not complied with the ACA may give notice directing compliance (s.121) or issue a formal warning to a person contravening a registered industry code (s.122). If there is no compliance, the Federal Court may impose a fine (Part 31, ss.569 to 572).

If an industry code has not been developed and/or the ACA has requested an industry code without success or has not registered the industry code, then the ACA may make an industry standard which is a disallowable instrument (s.123). Before determining or varying an industry standard the ACA must satisfy certain consultative criteria (ss.132 to 135). Where no body or association represents a section of the telecommunications industry the ACA may request, by notice in the Gazette, that if such a body or association came into existence then a request would most likely be made (s.124). Where no body or association comes into existence the ACA may make an industry standard which is a disallowable instrument (s.124).

Where an industry code is determined by the ACA to be *deficient* (that is, it does not provide appropriate community safeguards or does not adequately regulate the industry), then the ACA may make an industry standard (s.125). Where a registered industry standard is not complied with the Federal Court may impose a fine (Part 31, ss.569 to 572). The ACA may issue a formal warning to a person contravening a registered industry standard (s.129). An industry standard cannot apply until 180 days after 1 July 1997, that is, 1 January 1998 (s.127). The ACA may revoke an industry standard if it is replaced by an industry code (s.131).

The effect of these provisions is that privacy regulation may occur under the Act if:

- the telecommunications industries develop and register industry codes which are registered by the ACA and these codes address all the privacy concerns; or
- where there is no industry code or it is deficient, the ACA may implement industry standards addressing all privacy concerns where that does not affect design and performance of equipment, cabling, networks and facilities, unless the ACA determines that the community benefit outweighs the costs of compliance.

The Act also retains and extends some of the privacy protections that were enshrined in the previous *Telecommunications Act 1991*. These measures:

- protect confidentiality of information or a document that relates to the contents or substance of communications that have been or are being carried (ss.276, 277 and 278);
- protect information or a document that relates to the affairs or personal particulars (including any unlisted telephone number or any address) of another person (ss.276, 277 and 278);
- protect information or a document that comes to that person in their telecommunications business or employment (ss.276, 277 and 278);
- give exceptions for persons carrying out their employment, where disclosure is by authorisation of law, for law

enforcement and protection of the public revenue, for Australian Security Intelligence Organisation, when assisting the ACA, the Australian Consumer and Competition Commission (the ACCC) or the Telecommunications Industry Ombudsman (s.246), certain emergency service calls, threats to a person's life or health, certain maritime purposes, where there was consent and as specified by regulations (ss.279 to 302); and

- specify certain record keeping requirements over which the Privacy Commissioner has the function of monitoring compliance (ss.304 to 309).

Although this scheme seems detailed, there is a strict limit on the powers of the ACA. It cannot make industry standards with respect to privacy if the industry standard would be likely to affect, directly or indirectly, the design or performance of customer equipment, customer cabling, telecommunications networks or facilities, unless the community benefit outweighs the compliance costs (s.126).[8]

Australian Democrats' major concerns

The Australian Democrats believe personal information should be protected through a comprehensive national legislative scheme. This should be a strong, enforceable privacy protection which covers both the public and the private sectors with powers vested in an independent body to investigate and enforce its decisions based on clear principles of what constitutes a breach.

The *Telecommunications Bill 1997* was debated in both the Senate and the House of Representatives on the basis that the Government would be introducing a comprehensive privacy scheme applying to the private sector.[9] Such a scheme would have applied to the telecommunications industry and would have provided an incentive for the industry to develop codes of practice and comply with good privacy practices. This would have addressed many of the Australian Democrats' concerns. Without this scheme there are gaps in the privacy protection afforded to telecommunications consumers.

The scheme set out in the Act is not sufficient because:

- there are no legislated mechanisms for investigating a privacy breach;
- there are no legislated mechanisms for an individual to bring an action for breach of the industry code or industry standard, and this is of particular concern with respect to privacy, as it is likely to be an individual that has suffered the consequences of a privacy code or standard non-compliance;
- only the Minister, the ACA or the ACCC can bring an action in the Federal Court to recover pecuniary penalties under the *Telecommunications Act 1997* for the Commonwealth for contravention of an industry code or industry standard;
- the Federal Court is the first court or tribunal of appeal or review which will be both expensive and restricted by complex procedural rules; and
- there is no role for the Privacy Commissioner to exercise powers under the *Privacy Act* to investigate, determine and enforce privacy breaches.

The Privacy Commissioner should be central to privacy regulation and that role should be consistent with the Privacy Commissioner's functions as set out in the *Privacy Act*. This has been partly satisfied by requiring the Privacy Commissioner to be consulted in the registration of industry codes (s.112), the determining or varying of industry standards (s.134), the compliance with the existing legislated privacy protections with respect to record keeping in the Act (ss.304 to 308) and a general function to encourage corporations to develop programs for the handling of records of personal information that are consistent with the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data issued by the Organisation for Economic Co-operation and Development (s.27(1), *Privacy Act)*. However, the Privacy Commissioner is not included in any complaints, investigation or enforcement role. Without a comprehensive private sector privacy scheme this is a significant omission from the Act.

The Act sets up the mechanisms for a privacy scheme through the development of industry codes and industry standards, but these measures have left a gap in privacy protection. There are no registered industry codes in place that relate to privacy and the Act specifically prevents industry standards operating before 1 January 1998 (s.127). Until such industry codes or industry standards are registered there is effectively very limited privacy protection in the telecommunications industry.

The privacy measures in the Act are arguably directed at enforcing compliance with agreed industry codes and industry standards. The provisions do not relate to persons or organisations that have their privacy breached and there is no guarantee that either the industry or the ACA will implement such industry codes or industry standards. Even if industry codes or industry standards are implemented, there is no benchmark, such as an equivalence to the present *Privacy Act* which must be satisfied. In effect there are no guarantees for consumers that their privacy will be protected to the same standard as that applied to the public sector.

The ability of the telecommunications industry to be independently scrutinised by an aggrieved consumer and have some action taken by the industry where that consumer has a valid complaint is doubtful. Although the Act provides for a Telecommunications Industry Ombudsman (Part 10), the legislated powers of this position are very limited. Certain carriers and carriage service providers[10] are required to enter the Telecommunications Industry Ombudsman scheme which must provide for the Telecommunications Industry Ombudsman to investigate, make determinations and give directions relating to complaints about 'carriage services by end users of those services' (s.246). The term 'carriage services' is defined as 'a service for carrying communications by means of guided and/or unguided electromagnetic energy' (s.7). It seems doubtful the Telecommunications Industry Ombudsman can deal with privacy complaints because the complaint is unlikely to be 'about billing, or the manner of charging' (s.246(4)) alone. The Telecommunications Industry Ombudsman does not have the independence of the Privacy Commissioner (s.19, *Privacy Act)* or power to receive complaints about an 'act or practice that may be an interference with the privacy of the individual' (s.36, *Privacy Act),* to investigate complaints (s.40, *Privacy Act),* to obtain information, interview witnesses and refer matters to other authorities (ss.44, 45 and 50, *Privacy Act),* and to make a determination with enforcement powers (s.52, *Privacy Act)* which has the effect as an order of the Federal Court (s.55, *Privacy Act).*

Telecom/Telstra, as one of the major players, evolved in a culture of privacy protection up until 31 January 1992 when

it was bound by the *Privacy Act* . Thereafter it committed itself to the Information Privacy Principles (s.14, *Privacy Act),* developed internal privacy guidelines in conjunction with the Privacy Commissioner and established an internal Privacy Audit Panel. However, this has been a voluntary arrangement and has not been adopted by the other industry players. The new players have neither a track record of commitment to privacy or a culture of dealing with personal information. The Act does nothing to ensure this culture will evolve.

What business really wants

When the Prime Minister performed his 'backflip' on 21 March 1997 he said he was meeting the concerns of business: 'The Commonwealth opposes such proposals which will further increase compliance costs for all Australian businesses, large and small ... At a time when all heads of government acknowledge the need to reduce the regulatory burden, proposals for new compulsory regimes would be counterproductive'.[11] It is uncertain whether the telecommunications industry, or the business sector generally agrees with the Prime Minister.

The quantitative research in Australia is very limited. However, Price Waterhouse surveyed 130 large businesses (including the telecommunications industry) earlier this year and found 70% favoured, 10% were 'neutral' and 20% opposed the introduction of comprehensive national privacy laws. The survey report concluded: '... Australian business has identified privacy as a major business risk and they are looking to the Australian Government for guidance on how to manage it'.[12] This survey confirms an earlier survey conducted by the Faculty of Business and Economics at Monash University which found businesses recognise the importance of personal information to their clients and employees.[13] The Prime Minister's statement is also at odds with the major industrialised countries which have recognised the economic and social benefits (discussed below) of privacy protection.

In the absence of Commonwealth legislation the States and Territories are considering filling the void. New South Wales has clearly indicated it will. Victoria, Tasmania, South Australia, Queensland, the Australian Capital Territory and the Northern Territory are presently examining privacy legislation options. If State and Territory governments do introduce privacy schemes, businesses will be required to comply with each of those schemes which may be different for each State and Territory, therefore increasing overall compliance costs significantly. The Prime Minister's and Attorney-General's[14] reassurance about compliance costs and regulatory burdens are hollow in light of these State and Territory responses, and highlights the need for a national and consistent privacy scheme.

International perspective

Telecommunications are the way most Australians interact with the world, both in business and personally. Moves to limit or exclude Australia from international telecommunications will adversely affect Australia's telecommunication's industry in particular and Australians generally. Yet, Australia could be faced with this. The European Union Privacy Directive which comes into force on 1 July 1998 will prevent trade with Australia (and any other country) if there are not 'adequate' privacy laws to protect personal information. In a speech to a Banking Conference the Attorney-General stated that the European Union did not require 'identical protection' or 'equivalent protection', but rather 'adequate' protection.[15] This is true — but *no* protection at all is unlikely to be an 'adequate' level of protection. Without a clear regulatory privacy scheme, it may not be possible to satisfy the European requirements. It is possible each business agreement will need to be sanctioned or a special arrangement negotiated with each European State. This will significantly increase the compliance costs and regulatory burdens for businesses. A clear regulatory scheme compatible with this Directive will avoid the issue of what is 'adequate'.

The Ministerial meeting of G7 industrialised countries in February 1995 and APEC Ministers in May 1995 identified privacy as an issue which was important for commercial reasons. The European Union has adopted a legally enforceable law in the form of the Privacy Directive and New Zealand has implemented the *Privacy Act 1993,* which creates a comprehensive national privacy scheme applying to both the public and private sectors. The Government's Discussion Paper (discussed above) set out a scheme which was consistent with these international developments and international standards and would have met the concerns of the European Union Privacy Directive and our trading partners.

The speed and ease of telecommunications means that personal information is being increasingly collected, stored and processed. This personal information, and the right to its protection are gaining increased recognition and legislative protections. The telecommunications industry highlights these particular issues because of the almost universal involvement of telecommunications in our everyday lives. The European Union Privacy Directive's objective and purpose is 'to secure ... respect for his [and her] rights and fundamental freedoms, and in particular his [and her] right to privacy, with regard to automatic processing of personal data relating to him [or her]'. The term 'automatic processing' is broadly defined to include storage, alteration, retrieval, etc. Telecommunications are central to automatic processing in an international and domestic environment.

It is a fundamental principle that a person has a right to know what personal information is held about them, and if the information is lawfully held, that the information is correct. The International Covenant on Civil and Political Rights provides that 'no one shall be subject to arbitrary or unlawful interference with his [or her] privacy' (Article 17). The Universal Declaration of Human Rights provides that 'No one shall be subjected to arbitrary interference with his [or her] privacy, family, home or correspondence, nor attacks upon his [or her] honour and reputation (Article 12). Everyone has the right to the protection of the law against such interference or attacks'. Privacy *is* a human rights issue and the Government should deal with the issue as a part of Australia's international human rights obligations. These are fundamental human rights set out in Agreements to which Australia has attested and the domestic laws should reflect this international commitment.

The issue of Australia's international obligations and the Government's willingness to legislate to recognise these commitments is further highlighted by legislation like the *Trans-Tasman Mutual Recognition Bill 1997* which is presently before the Senate. This legislation is aimed at enacting domestic laws which conform to Australia's treaty obligations with New Zealand under the Trans-Tasman Mutual Recognition Agreement. The Agreement is directed to removing barriers to goods and occupations between Australia and New Zealand. This legislation includes specific provi-

sions about privacy which ensure that personal information provided to authorities registering an occupation protect the privacy of that information. This is the recognition in domestic law of an Agreement between Australia and New Zealand. The same measures should be taken to recognise the right of privacy set out in the International Covenant on Civil and Political Rights and the Universal Declaration of Human Rights.

What of the future

In its present form, and without the benefits of a private sector privacy scheme, the Act relies heavily on the corporate citizenship of the telecommunications industry. The Attorney has said that business has a commercial incentive to protect privacy[16] and Minister Amanda Vanstone has said that some businesses have already taken steps to introduce good privacy practices.[17] The privacy measures in the Act and a reliance on corporate citizenship are steps in the right direction, but it should not be the only means of regulation. The Australian Democrats support a strong and enforceable national privacy scheme which goes to assuring consumers that their personal information is adequately protected. Corporate citizenship alone falls short because it does not have the supporting mechanisms for investigation and enforcement which are necessary elements in ensuring any privacy scheme is complied with. The benefits to telecommunications consumers are likely to be considerably less than if the Government had extended the *Privacy Act* to the private sector.

The Australian Democrats would like to see a scheme where industry is either covered by legislated privacy principles or develop their own codes of practice with the co-operation of the Privacy Commissioner which are tabled before the Parliament as disallowable instruments. The codes of practice should maintain comprehensive and enforceable privacy protection with powers conferred on the Privacy Commissioner which are similar to those presently set out in the *Privacy Act*. This is essential to keep pace with the developments in other countries and the advances in information collection and exchange technology. The telecommunications industry and consumers are likely to benefit from such a scheme, through continued access to the world telecommunications business and the confidence of consumers that their personal information is adequately protected.

References

1. Wright, C., 'Banks tapping into heavy number crunching', *Australian Financial Review*, 26 May 1997.
2. Online Policy Statement, Coalition Election Papers, 1996.
3. Law and Justice Policy Statement, Coalition Election Papers, 1996.
4. 'Privacy Protection in the Private Sector', Discussion Paper, September 1996, Commonwealth of Australia.
5. Attorney-General and Justice Minister, Press Release 142, 12 September 1996.
6. 'Privacy Protection in the Private Sector', above, at p.13.
7. Prime Minister, Press Release, 21 March 1997.
8. It is interesting that s.115(3) specifically excludes the operation of s.115(1). The effect of this provision is to leave open the development of industry codes for privacy and industry standards for privacy where the community benefit outweighs the compliance costs, although industry codes can only be made by industry. There is no equivalent to s.124 which applies to an industry code.
9. The Senate passed the *Telecommunications Bill 1997* (and other telecommunications legislation) with amendments on 24 March 1997. The Bill was returned to the Senate from the House of Representatives on 26 March 1997. The Bill was assented to on 22 April 1997 with various sections coming into force at different times. The sections concerned with privacy came into effect on 1 July 1997.
10. Section 7 defines 'carrier' as the holder of a carrier licence under s.56, and 'carriage service provider' as a person who supplies carriage services as set out in s.87.
11. Prime Minister, Press Release, 21 March 1997.
12. Privacy Survey 1997, Price Waterhouse, 215 Spring Street, Melbourne, Victoria, 3000.
13. Boykett, J., O'Reilly, H. and Tucker, G., 'Private Sector Attitudes to Information Privacy', 1996, 3 *PLPR* 101.
14. van Leewen, H., 'Lack of privacy safeguards won't "affect EU trade"', *Australian Financial Review*, 23 May 1997.
15. van Leewen, H., above.
16. van Leewen, H., above.
17. Hansard, 13 May 1997 p.3000.