JG5Jun:A00/186
Enquiries: Mr. Gaudin
Telephone: 9268 5581

The Secretary
House of Representatives Standing
Committee on Legal and Constitutional
Affairs
Parliament House
CANBERRA ACT 2600

5 June, 2000

Dear Ms Cornish,

Thank you for your invitation to make a submission on the Privacy Amendment (Private Sector) Bill 2000. Attached is a submission which considers selected aspects of the Bill.

Owing to competing priorities I am not in a position to make as comprehensive submission at this time as I would have wished. I have sought to focus on those issues which reflect my office's experience of legislation with both public and private sector coverage in New South Wales.

I also attach copies of previous submissions made to the Commonwealth Attorney-General in relation to the release of the information paper and key provisions.

I would naturally be happy to enlarge on any of the issues

Yours sincerely,

Chris Puplick
Privacy Commissioner

Privacy New South Wales

Submission to the House of Representatives Standing Committee on Legal and Constitutional Affairs on the Privacy Amendment (Private Sector) Bill 2000

Privacy NSW, the office of the New South Wales Privacy Commissioner, was established in February 1999 under the Privacy and Personal Information Protection Act 1998. My office replaced the New South Wales Privacy Committee, which was created in 1975 and which represented one of the earliest legislative responses to an upsurge of concern about privacy over the previous decade. The Committee was originally set up as a result of recommendations in a 1973 report prepared by the late Professor W L Morison which recommended a representative body to further study and make recommendations on what governmental action was needed to protect privacy. Membership of the Committee drew on expertise from the public and private sectors, politics, law and universities.

The subsequent evolution of the Committee illustrates the way concerns over privacy have evolved over almost 30 years. This submission is grounded in this experience.

From the outset the Committee assumed a dual function. It initiated research into privacy issues with particular emphasis on the record keeping activities of New South Wales public sector bodies. It also assumed the role of a privacy ombudsman, investigating and resolving complaints relating to individual breaches of privacy in both the public and private sectors. The Committee dealt with complaints by providing telephone advice and investigating and reporting on formal written complaints. The Committee also prepared reports, issues papers and guidelines based on contentious issues identified through complaints. The continuation of the Committee from 1975 to 1999 testified to the continued need for a body capable of authoritatively addressing the varied range of privacy issues.

Many of the issues taken up by the Committee have been incorporated into other areas of legal and administrative reform, for example specialised investigation bodies in the health and community welfare sectors, and reform of the law dealing with video surveillance and spent convictions. The Committee was an early supporter of freedom of information as a means for individuals to access their own files held by government agencies. It promoted a self regulatory regime in consumer credit reporting which ultimately led to the credit reporting provisions of the current Commonwealth Privacy Act. Its policy positions have been incorporated in the guidelines covering New South Wales public sector employment.

The Committee's early experiences with the shortcomings of self regulatory privacy protection particularly in the area of credit reporting led it to advocate comprehensive information privacy legislation from 1982. Popular support for privacy protection has been widespread during the past decade. However substantial legislative achievement has been slow and limited. The Commonwealth Privacy Act of 1988 covered the Federal public sector. New South Wales public sector legislation took another decade. There has been talk, but no legislation in other states. It may be useful to understand some of the reasons for this disappointing progress.

One explanation is that privacy protection loses out in the confrontation between a diffusely held public interest and the specific and concentrated interests of particular businesses and administrative agencies. Where privacy legislation is passed it often takes the form of a brief concession of a right, followed by a lengthy list of exemptions. An example is the Telecommunications Interception Act, which has one subsection prohibiting the interception of people's phone calls and 108 sections detailing how interception can be performed legally.

The current Bill reflects this pattern with its complex range of exemptions for specific entities and activities.

Another explanation refers to the adversarial nature of Anglo-American law. It appears to be difficult to draft legislation to protect something as intangible as personal information without appearing to interrupt the free flow of information or handicap legitimate information processing. This has led to many organisations seeking to exempt themselves from proposed privacy laws rather than having to face the uncertainty of regulation. It also leads to exemptions which are expressed in broader terms than necessary to safeguard legitimate commercial or administrative operations.

The impetus for comprehensive information privacy protection has tended to come from European states which are more comfortable with a codified and flexible approach to the expression of legal rights and responsibilities. The United Kingdom has achieved information privacy law largely through pressure from its European neighbours. Public concern about privacy in the United States has been high but has tended to produce limited sectoral legislation leaving major gaps in coverage.

The impetus for New South Wales privacy legislation came from an investigation and report by the New South Wales Independent Commission Against Corruption in 1991-1992 which highlighted a widespread illicit trade in information mostly of a personal nature from government sources. The ICAC was primarily concerned with the opportunities this trade provided for the corruption of public officials. However it was obvious that a more systematic and above the board approach to the release of government information would involve privacy considerations. Further pressure has come from restrictions or proposed restrictions on transborder data flows in privacy legislation adopted by countries which trade with Australia, most particularly those European states who are bound by the European Union's Data Protection Directive.

The New South Wales Privacy and Personal Information Protection Act was passed in 1998. Substantial provisions only come into force on 1 July 2000. The legislation covers New South Wales public sector agencies including local councils and universities. It does not seek to cover non-government service providers who exercise functions on behalf of public sector agencies, but does provide for the possibility of gazetting non-government data service providers as public sector agencies.

The current Bill is the outcome of a process which began in 1996 with the Commonwealth Government's Discussion Paper, *Privacy Protection in the Private Sector*. After the Prime Minister's decision in March 1997 to postpone legislation, the then Federal Privacy Commissioner commenced a consultation process leading to the development of *National Principles for the Fair Handling of Personal Information,* issued in January 1999. These principles form the basis of the National Privacy Principles in the current Bill.

As a consequence of the slow and sometimes tortuous path towards comprehensive information privacy legislation it is possible to lose sight of the reasons for privacy protection.

- Privacy is a right and not simply a convenient piece of commercial window-dressing.
  .

- At the same time, privacy legislation offers tangible benefits to businesses and other users of personal information by offering clear and authoritative standards through which they can secure the confidence of their clients, customers and staff.

- There should be a clear idea of what privacy legislation seeks to achieve, the kind of strategies which are needed to achieve it and possible pitfalls, such as overly general exemptions which will frustrate its intention.

- To work effectively legislation needs to be clear, consistent and comprehensive rather than providing a baffling maze of alternative remedies and exemptions.

- Legislation needs to achieve a cultural shift so that organisations and their staff can feel comfortable and confident in the way they handle personal information and customers and clients can have consistent and realistic expectations.

I am not convinced that the Bill in its present form provides the clear and consistent model which is needed to the extent that:

1. it perpetuates a distinction between public and private sector instrumentalities which is becoming increasingly irrelevant and which in some contexts will lead to regulatory blind spots;

2. it provides a complex framework of exemptions which work against individuals developing clear privacy expectations in their dealings with agencies and organisations;

3. organisations which need or wish to demonstrate their privacy credentials will be excluded from coverage;

4. key provisions are lacking in precision in a way which risks the creation of significant loopholes which will frustrate the effectiveness of legislation;

5. broader than necessary exclusion of key areas such as employee records, political parties and the media sends messages which are inconsistent with the aims of privacy legislation and undermines the ability of the Bill to deliver broad, non-sectoral information privacy protection

Privacy Principles

The attempt to separate privacy issues according to whether they relate the public or private sectors becomes increasingly artificial as the activities of the two sectors increasingly cross-over. Public sector agencies are subject to revenue pressures to market their services to customers and to provide information held on government databases to commercial interests. Private sector firms are increasingly involved in the delivery of public services and in managing outsourced public sector operations. Increasing convergence of computer and telecommunications technology increases the flow of information between sectors.

Under the Bill, the Federal public sector will still have to comply with the *information privacy principles* in section 14 of the Privacy Act. Eligible non-government organisations will comply with the National Privacy Principles. These principles were developed as the centrepiece of a voluntary self-regulatory regime. In some respects they reflect the more informal processes of

private business. In other respects they mark a distinct improvement on the information privacy principles to the extent that they address new issues such as anonymity, the use of common identifiers, sensitive classes of personal information and transborder data flows.

The New South Wales Privacy and Personal Information Protection Act 1998 incorporates a set of *information protection principles* which are substantially similar to the existing Commonwealth Privacy Act's information privacy principles. They are substantially modified by a wide range of exemptions. The Act also provides for the development of privacy codes of practice which are different from the privacy codes proposed in the Bill, in that they are not intended to replace the default regulatory scheme but simply serve as a way to tailor individual principles to the needs of a specific agency or activity.

As a result of these different sets of principles, individuals wishing to pursue their privacy rights will have to navigate around subtle technical differences according to whether they are dealing with a federal, state or non-government organisation. In the medium term this seems unavoidable. Within the current legislative timetable it would be unrealistic to achieve a single set of principles. I would certainly not support assimilating the National Privacy Principles to the older and less flexible principles which apply to public sector agencies. However some of my criticisms of the Bill are directed against the perpetuation of the artificial distinction between public and private sector privacy.

I have distinct reservations about some of the individual National Privacy Principles as follows.

Principle 2.1(c) should be amended to make it clear that it permits the use of information for direct marketing by the collecting organisation and not disclosure to another organisation for such use without prior consent.

The exemption for use or disclosure of health information for research or statistical use (2.1(d)) is too broadly expressed and leads to a class of information regarded by most people as particularly sensitive having less protection than other kinds of personal information.

The exemption for use or disclosure of information which an organisation believes is reasonably necessary for the protection of the public revenue (2.1(h)(iii)) is too broadly expressed and inappropriate in a private sector context. Governments should rely on their ability to invoke specific laws to require disclosure for this purpose.

A number of the principles rely on consent by individual information subjects to handling their personal information in specific ways (principles 2.1(b), (c), d(i), 2.4(a)(i), 10.1(a)). These provisions can only effectively deliver privacy if individuals have sufficient information to understand what uses of their information they are consenting to. One significant difference between public and commercial private sector agencies is that the latter generally deal with clients or customers on the basis of an up-front contract. My office has come across instances of business contracts which, in purported compliance with privacy policies, have asked customers to consent in advance to any use of their personal information. This effectively precludes the provision of sufficient information about proposed uses or any negotiation by the customer over individual details or disclosures. I am concerned that organisations will be encouraged to adopt the same approach under the Bill.

The definition of consent in the Privacy Act merely states that it may be implied or express. Section 27(1)(e) of the Act which gives Privacy Commissioner power to make guidelines for the avoidance of interferences with privacy by agencies is to be extended to organisations. The Privacy Commissioner's *Plain English Guidelines to Privacy Principles 8-11*, Guideline No 15 address the issue of consent. It emphasises the need for consent to be free and informed

in a way which would contradict broad waiver provisions, were the same approach to be extended to the National Privacy Principles. I would nevertheless question whether non-enforceable guidelines would provide sufficient protection against the use of general waiver terms.

I recommend tightening the Act's definition of consent to require it to be informed, or including an explicit provision to discourage organisations from contracting out of their privacy obligations.

A further concern relates to the transitional provisions which will apply to the principles under proposed section 16C. Principle 2 dealing with use and disclosure will not apply to personal information collected before the commencement of the Part. This creates serious practical difficulties for organisations seeking to determine which elements of an ensemble of information about a particular individual are covered. They will need to stream specific items of information or engage in complex and artificial analysis to determine the extent of their liability under the Act.

This cut-off date also seems largely unnecessary. Restrictions on use or disclosure are hardly so severe as to require distinctions based on the time of collection. Significant industry sectors already claim to adhere voluntarily to privacy principles. Other organisations will have ample warning to get their houses in order. The proposed complaint investigation mechanism can easily accommodate time issues by considering what conduct is reasonable. Where an organisation is genuinely handicapped in relation to a permissible use of information because it was not required to comply with the principles at the time the information was collected it would be a simple matter to deem the appropriate notification or consent in the Act.

Enforcement Issues

Along with the different sets of principles the Bill will contribute to a variety of methods by which people can enforce their rights to privacy. Although enforcement under the Bill relies primarily on complaints by aggrieved individuals, the provisions to assist people in knowing how to complain are weak.

Under the New South Wales Act enforcement of the information protection principles is largely the responsibility of individual public sector agencies. Agencies which receive written applications alleging a breach of a principle, code or public register provision must conduct an internal review of the conduct and report to the applicant. The applicant can then seek a further review by the Administrative Decisions Tribunal. My office has a right to be informed of applications for review and to make representations at both levels of review.

Individuals can make a complaint to the Privacy Commissioner about the activities of non-government agencies or can choose to have a complaint against a public sector agency investigated by the Privacy Commissioner but without the remedies which are available through the system of internal and external review. This dual approach to complaint handling has certain advantages. My office remains a point of contact and advice and is able to monitor areas of friction. At the same time agencies have an incentive to comply with the privacy requirements and respond immediately to complaints.

Complaints about Commonwealth agencies and credit reporting are made to the Federal Privacy Commissioner. The Commissioner also conducts compliance audits and approves or issues guidelines covering specific activities. Under the Bill the Commissioner will also receive

and investigate complaints against eligible organisations which are not subject to a privacy code or where the code nominates the Commissioner s independent adjudicator.

Currently the federal Privacy Commissioner strongly encourages complainants to resolve their differences with the agency before lodging a complaint with his office. Proposed section 40.1A will reinforce this process for private sector complaints which the Commissioner has the power to investigate.

Where a code under the Bill provides for an independent adjudicator complaints will have to be directed to that person or body. It seems reasonable to assume that sectors such as banking and insurance which already have self regulatory complaint handling schemes will seek to assimilate their privacy code adjudication to such schemes, under which complaints have first to be lodged with the bank or insurer. Unfortunately the track record of these schemes does not inspire confidence that complainants will be adequately informed of their right to have a complaint processed in a scheme which provides for independent review.

The National Privacy Principles should be amended (principles 1.3, 5 and 6.7) to ensure that an organisation notifies people of their rights to independent adjudication either by the Commissioner or the code authority.

Exclusions

Small Business

My main concern in relation to this exemption relates to its complexity. Individuals wishing to establish the scope of their privacy will be presented with a confusing set of conditions and options. Businesses and non-government organisations wanting to assure their customers and clients that they take their privacy rights seriously will be left in limbo if their turnover is under $3 million. Organisations will move in and out of the small business category depending on their turnover for the previous year. Delinquent businesses which minimise their tax liability will be rewarded through exclusion from the privacy scheme.

The exclusion from the small business category for organisations which collect or disclose personal information for a benefit (6D(4)(c) and(d)) is so obscurely expressed that I have difficulty in determining what end it is intended to achieve or what kind of businesses it will exempt. It invites organisations to adopt avoidance strategies in the way they charge for their services. Businesses which generate a large number of privacy complaints to my office, such as the Tenancy Reference Services may avoid coverage because the way they charge for their activities cannot be brought under this provision.

I expect that the effect of these exclusions will increase the pressure on my office to deal with privacy complaints from the non-government sector in New South Wales, but without the remedies which the Bill will provide.

An alternative would be to give the Federal Privacy Commissioner the power to make a code for small business which businesses concerned to demonstrate their privacy credentials could opt into.

State trading enterprises

The New South Wales privacy legislation excludes State owned corporations (SOCs), which derive their corporate status from being listed in Schedule 5 of the State Owned Corporations

Act 1989, rather than from incorporation under the Corporations Law. This exclusion was based on the assumption that private sector organisations which compete with government trading enterprises would be excluded from privacy legislation or that subsequent Commonwealth private sector legislation would apply to SOCs, thus maintaining a common regime for commercial enterprises. In fact proposed section 6C(1) & (3) of the Bill leaves SOCs in a position where they are not covered by either state or Commonwealth privacy legislation. I understand that the Commonwealth Attorney-General is of the view that there would be constitutional difficulties to ensuring coverage of SOC's by the Bill. I propose to make representations to the New South Wales Government to resolve the uncertain status of SOCs.

Contract Service Providers

The artificiality of the distinction between public and private sector privacy is reflected in the confusing coverage of contracted service providers performing Commonwealth contracts. The intention of the provisions is to avoid conflict between the National Privacy Principles and contractual provisions imposed by agencies in conformity with the information privacy principles. The relevant provisions are complex and it is unnecessary for me to reach a concluded view as to whether contractors are adequately covered under them. It appears that an organisation which is covered by the National Privacy Principles cannot be investigated under a code for performance under the contract which is inconsistent with the code, but may be investigated by the Privacy Commissioner if the conduct which breaches the contract.

The exclusion of businesses performing contracted services for state authorities will leave organisations in New South Wales largely uncovered, given that, in most instances they are not be required to comply with the mandatory compliance provisions or review under the New South Wales Privacy and Personal Information Protection Act. It is not clear that the remedies an aggrieved individual can obtain from the public sector agency which contracts with the service provider will adequately deal with the kind of privacy issues which may arise. However, as with the state trading enterprises, I accept that it may be difficult to remedy this situation under the Bill without creating risks of conflict between state and federal legislation.

Political Parties

Proposed section 7C excludes political acts and practices of political parties and their agents at Commonwealth, State and local level in relation to their participation in elections, referenda or other aspects of the political process. I have greater difficulty in accepting that there is any ethically defensible basis for such a comprehensive exclusion. Parties and politicians engage in particularly intensive and controversial processing of personal information. To exclude these activities in their entirety sends the contradictory message that politicians do not care to be bound by the same kind of standards they propose to impose on other sections of the population. It implicitly denies that privacy is an individual right.

It should be possible to address any concerns about privacy obstructing the political process by more narrowly designed exemptions to specific principles such as those dealing with access, use and sensitive information. For example principle 10 (d)(i) could be expanded to include people who have contact with a political party in relation to its political activities.

Media and journalism

An expansive exemption for the media also sends mixed messages about the Bill's commitment to privacy. While I would probably concede that information privacy legislation is not the most appropriate way to deal with the more egregious media invasions of privacy, media organisations are now involved in a wide range of information processing and delivery

activities, many of which are only indirectly related to the dissemination of news and journalistic opinion. The combined effect of the way journalism and media organisation are defined in sections 18 and 19(6) to broadly cover the activities of collecting or preparing of information for dissemination or disseminating it to the public is far wider than necessary to protect the freedom of expression through the media. It will creates a large hole in any scheme for information privacy protection. It would for example appear to cover any organisation which collects and disseminates personal information over the Internet, presumably including the kind of criminal record information which is currently being made available on the CrimeNet web site.

The exemption should be narrowed to focus on the traditional news gathering, reporting and broadcasting functions of the media.

I would also query whether the undefined word journalist in new section 66(1A) will begiven an expanded meaning as a result of the way journalism is defined, thus expanding the shield provision to, for example, any person who collects information for the purpose of posting it to a web site.

Employment Records

I am concerned that this exemption will in fact have a much broader impact on employees expectations of privacy than may appear at first sight. The category of employee records is capable of indefinite expansion because of the way that technology in the workplace generates an increasing amount of information about employee behaviour and performance. For example recent concern about privacy rights in relation to employee e-mail would appear to be caught by this exemption.

A broad exclusion of privacy rights in employment sends the wrong message to employees who will be in the forefront of implementing privacy policies on behalf of an organisation. It runs counter to widely held expectations in relation to privacy and transparent processes in the workplace which are reflected by complaints and inquiries to my office.

There may be a case for protecting certain classes of employee information from access, for example confidential references and ongoing disciplinary records or material to justify dismissals. This should be achieved by an appropriate modification of the principles, rather than a general exemption.

I note the Attorney-General's view that handling of employee records is a matter best dealt with under the Workplace Relations Act. I would like to be satisfied that effective legislation will be passed in this context, before accepting that this resolves the issue.

Conclusion

I have not been in a position to address all the issues raised by the Bill. It can hardly be said, as its objects clause states, to establish a single comprehensive national scheme to cover the handling of personal information. It may very well reduce the level of privacy protection we currently enjoy, for example by legitimising secondary uses of information in critical areas such as health, revenue protection and law enforcement. I recommend that the Committee carefully scrutinise it and seek appropriate amendments.

Attachment

Privacy NSW's private sector coverage.

Privacy NSW operates a public advice and inquiry service dealing with a wide range of privacy issues.

In the six months between 1 July 1999 and 31 December 1999 we recorded the following calls.

Subject of call	Advice	Complaints	Total
disclosure	103	106	209
general privacy information	180	7	187
surveillance	73	59	132
collection of personal information	42	47	89
criminal records	54	16	70
marketing and surveys	22	35	57
credit and finance	33	22	55
housing and tenancy	11	43	54
obtaining access to my records	35	18	53
telecommunications and Internet	24	22	46
medical and health records	15	8	23
media and publishing	8	8	16
legal and courts	2	7	9
	602	398	1000

This period was chosen as:

- it represents the first full half year when Privacy NSW was operating under its new investigative functions;
- there is a reasonably typical cross-section of issues, more recent months reflect a greater proportion of inquiries on compliance with the new public sector provisions;
- the number of calls recorded happens to facilitate calculation of percentages

Because respondents are not always identified it is not possible to give a reliable breakdown according to whether organisations whose conduct is queried or complained about are in the public or private sector. However certain categories of complaints such as housing, credit, media and marketing are all predominantly private sector oriented. Calls relating to employment issues are strongly represented under surveillance, criminal records, and telecommunications and Internet.

Not all calls which involve a complaint result in investigation by the Commissioner. The lack of effective remedies where a complaint is made in relation to employment acts as a disincentive

to people who are concerned to keep their job or find a new one. Over the same period Privacy NSW opened 176 complaint files. Major private sector issues included

marketing and surveys	17
tenancy related complaints	15
private employment	10
disclosure of financial information (non-credit)	9