

Overview

Introduction

Privacy has been a significant national and international concern for over 30 years. During the 1960s and 1970s a range of concerns about the relationship between citizen and state emerged with the perceived growing threat of large computer databanks. The 1980s saw significant efforts at international privacy standard setting and legislative efforts to provide adequate protection to privacy with 1984 a favourite time for reflection on technological challenges to individual privacy. The 1990s have seen technological advances undreamed of by George Orwell with the worldwide linking of computers, the electronic tracking of consumers and citizens and advances from the microscopic work of the Human Genome Project through to global satellite surveillance from outer space.

Together with the unease at entering a “brave new world” there remain a host of routine, but hugely important, privacy issues in everyday lives. Issues revolving around the information held on personnel files. The maintenance of blacklists in employment and housing. The accuracy of information upon which credit decisions are made. The wish to have our homes secure from unwanted intrusions.

It is into this environment that the Privacy Act 1993 was enacted. The Act covers a variety of matters as will be apparent from reading this report. Two central features are the establishment of a Privacy Commissioner and a set of information privacy principles. The Privacy Commissioner is an independent official. One function is to periodically review the operation of the Act. It is upon that task that I have been engaged in preparing this report. The information privacy principles apply to all agencies in the public and private sectors and govern the collection, holding, use and disclosure of personal information. Individuals have certain entitlements under the Act including to access and seek correction of personal information held by agencies and to obtain redress for interferences with their privacy.

The privacy regime established by the Privacy Act accords with obligations assumed by New Zealand as part of its membership of the United Nations and OECD. The Act follows well established models in Europe, North America and Australia, although it has a number of advanced features relating to its private sector coverage and its application to all personal information. It is noticeably less bureaucratic than early European models.

The Act has notably advanced the position of individuals in New Zealand in just a few short years. It is sometimes easy to forget quite how far we have come. For example, note:

- New Zealanders can access their own medical records. One might reflect upon the fact that individuals do not have this right in most parts of Australia and North America.
- New Zealanders are entitled to seek correction of information held on credit reporting agencies’ files if it is inaccurate. There was no right even to see the information prior to 1993.
- People may have access to information held on their personnel file. This has been an entitlement for employees in the public sector since the 1980s but it has only been

with the enactment of the Privacy Act that all employees enjoy this important right.

- Before the Privacy Act businesses and government agencies did not have to be open as to what they wanted personal details for and who they were going to share these with.
- Problems in other jurisdictions have not arisen here. For example, Australian lawyers report a lack of remedy for tenants wrongly placed on housing black lists.
- A simple complaints mechanism with an ombudsman-like investigation of privacy complaints with a non-adversarial approach.
- Outsourcing and privatisation do not deprive citizens of privacy rights in relation to personal data previously held by government agencies.

The report which follows examines provisions in the Act in detail and makes a number of recommendations. The purpose of the introductory and background material is to give an overview as to the context in which the Act operates and to introduce a number of the 154 recommendations.

REVIEW PROCESSES

Section 26(1) requires the Privacy Commissioner to review the operation of the Act as soon as practicable after the Act has been in force for three years and thereafter at intervals of not more than five years. The Commissioner's review concludes with a report to the Minister of Justice of the findings with recommendations as to any necessary or desirable amendments to the Act.

Section 26 does not require the review to be conducted in any particular way. However, I decided that it was desirable to consult with those affected - not just with government and business but with the public as well. I told the Minister of Justice of my intentions and a statement to this effect was made by the Minister in Parliament in August 1996.

Commencement of the review

Preparatory steps were taken during 1995 and the first half of 1996. Enquiries were made of overseas Commissioners as to recent reviews of their own legislation. A study was made of notable features of overseas laws and recent international instruments. In August 1996 I wrote to the chief executives of Government departments seeking ideas for the review and their initial impressions of the Act's operation. In January 1997 a similar letter went to 10 representative bodies in the private sector. In February a questionnaire concerning Part X of the Act was circulated to agencies participating in authorised information matching programmes.

The public phase of the review started at about the time of the Act's fourth anniversary with the submission of this report to the Minister of Justice soon after the fifth. While my review has been under way there have been a number of continuing developments needing study. These have included:

- European elaboration of the implications of the EU Directive on Data Protection;
- a number of Complaints Review Tribunal decisions following the end of the three year transition period;
- a procession of reviews and legislative proposals in Canada and Australia.

Discussion papers

Many people with useful experience with the Act might have been discouraged by a single large consultation document. So my office released 12 short discussion papers over a period of several months allowing people to choose to contribute depending upon where their experience or interest lay. The first eight papers corresponded to relevant Parts of the Act while the balance took the themes of compliance and administration costs, interaction with other laws, intelligence organisations, and new privacy protections. They primarily drew upon ideas and issues generated or identified within my office or in responses to the earlier letters to departments, representative bodies and the information matching questionnaire.

FIGURE 1. DISCUSSION PAPERS AND NUMBERS OF SUBMISSIONS

No	Title	Month released 1997	Submissions received
DP1	Structure and scope	July	47
DP2	Information privacy principles	August	47
DP3	Access and correction	August	50
DP4	Codes of practise and exemptions	August	21
DP5	Public register privacy issues	September	31
DP6	Complaints and investigation	September	29
DP7	Information matching	September	13
DP8	Law enforcement information	July	31
DP9	Compliance and administration costs	September	27
DP10	Interaction with other laws	August	34
DP11	Intelligence organisations	August	25
DP12	New privacy protections	September	27

A good response was received to the discussion papers and the list of those who made submissions is set out in Appendix B. Submissions continued to be received beyond the closing date of 10 November 1997 but most were to hand by February 1998. The submissions were acknowledged, numbered and compiled into four volumes. These were provided to the Ministry of Justice in February 1998 and were then made available for inspection or purchase from my office.

In November 1997 I held a series of consultation meetings in the four main centres. These enabled people who had made written submissions to elaborate upon issues of concern. A further series of meetings between myself, my staff, and certain invited experts, were held during December. Details are given in Appendix A. A consultation meeting was held with local authorities.

Completion of the report

During 1998 I continued to study the submissions and research the issues raised. In some cases further details were solicited from the person making the submission. In other cases, specialist drafting or technical advice was taken.

As material was prepared I took the opportunity to further consult people with relevant expertise and some agencies which might be specifically affected by recommendations under consideration. Most of the report was written by the end of July 1998.

THEMES IN THE REPORT

Although I consider the Privacy Act is firmly “on the right track”, I make 154 recommendations. It should not be inferred from the number of recommendations that the Act needs any major change of direction. There are proposals to rewrite provisions to make the Act more effective or understandable. Some new rights should be conferred or existing rights extended. I have proposed restrictions in the Act where I believe this will result in compliance cost reductions without significantly diminishing privacy rights. However, many of the recommendations can be characterised as being of a technical or “fine tuning” kind. Nonetheless, some of the 154 recommendations do raise matters of importance.

The recommendations in the report may be categorised in a variety of ways. A simple categorisation is used in the report itself, which examines the Act Part by Part, by linking the recommendations to the sections to which they relate. Accordingly, a reader interested in the relevant recommendations concerning access to personal information will find them in the part of the report relating to section 6 (information privacy principle 6) and sections 27 to 45. Those interested in recommendations concerning privacy officers will look at the material concerning section 23.

There are a number of themes in the recommendations:

- coverage of the Act;
- enhancement of individual rights;
- effectiveness of my Office;
- interaction with other laws;
- compliance and administration costs;
- ease of use of the Act;
- “adequate protection” in terms of the EU Directive.

The recommendations referred to in the following material are not exhaustive and many have been abbreviated and paraphrased.

Coverage of the Act

A principal feature of the Act is its broad coverage:

- it covers all “agencies” whether in the public or private sectors; and
- it applies to all “personal information”.

Broad coverage gives confidence that the information privacy principles apply in nearly all circumstances. The greater the inroads into the types of agencies or information covered, the greater the possibility of privacy being left unprotected. The broad coverage of the Act is also the surest guarantee that our law will be considered to offer “adequate protection” in respect of the tests established in the EU Directive on Data Protection. It also avoids compliance costs, creates certainty, avoids demarcation disputes or gaps between codes of practice.

Coverage is not absolute. There are bodies which are expressly excluded from the definition of “agency”. There are also partial exemptions applying to particular classes of agency or information. I examined the existing coverage of the Act to see whether changes should be made to extend or restrict the coverage.

Some recommendations are:

- the exemptions applying to the House of Representatives and MPs should be considered by a committee of Parliament - recommendations 5 and 6;
- consideration should be given to replacing the Parliamentary Service Commission’s total exemption with a partial exemption - recommendation 7;
- the partial exemption for the Parliamentary Service should be repealed or further restricted - recommendation 8;
- the exemption for the Ombudsmen should be repealed - recommendation 10;
- consideration should be given to narrowing the Royal Commission exemption - recommendation 81;
- the domestic affairs exemption should be restricted where an individual falsely represents the position to an agency - recommendation 82;
- the partial exemption for intelligence organisations should be further narrowed - recommendation 83;
- the IRD’s exemptions in section 101(5) and information matching rule 6(3) should be limited - recommendation 126.

There has been considerable interest in the exemption which applies to the news media in their news activities. I propose no change. The exemption is discussed at various places in the report in particular at paragraphs 1.4.49 to 1.4.62 and at paragraphs 4.4.49 to 4.4.55.

Enhancement of individual rights

The objective of the privacy law is to “promote and protect individual privacy”. I have examined the Act to consider whether it is effective in that respect and make a number of recommendations to better promote and protect privacy by enhancing individual rights and entitlements.

The 12 information privacy principles, and other controls relating to public registers and information matching, are at the heart of the Act. Aspects of the regime can be modified in certain ways by codes of practice. Through a mixture of constraints on agencies and entitlements for individuals these provisions establish a framework to protect individual privacy rights.

In the review I have studied ways in which privacy rights for individuals can be enhanced consistently with the international approach to the protection of privacy while taking account of competing interests. Few of the enhancements that I propose are entirely novel. Most involve adjustments to existing entitlements or the borrowing of ideas from international or overseas initiatives. In a number of cases I suggest specific entitlements consistent with the existing general entitlements. For example, I make proposals to change the information privacy principles and public register privacy principles to address direct marketing issues. Although the specific provisions will be new they will give effect to an objective of the existing principles - constraining a secondary use of information without the knowledge or authorisation of the individual.

Some recommendations are:

- allowing codes of practice to confer certain further entitlements - recommendations 18, 27, 35(b);
- requiring compliance with principle 3 where personal information is being collected directly from an individual for research or statistical purposes - recommendation 21;
- amending principle 7 so that agencies are obliged to inform requesters of their correction statement entitlements - recommendation 24;
- conferring an entitlement to require personal information to be deleted from direct marketing lists - recommendation 25;
- establishing entitlements to access information held by a private sector agency as a legal right in cases of private prosecutions - recommendation 36;
- requiring a requester to be given, without having to ask, the grounds in support of the reasons for withholding evaluative material - recommendation 54;
- requiring agencies to make reasonable endeavours to process urgent requests with priority - recommendation 67;
- allowing individuals to ask that their access requests not be transferred - recommendation 68;
- conferring further entitlements in respect of personal information held by intelligence organisations - recommendation 83;
- constraining bulk release of personal information from public registers for direct marketing - recommendation 91;
- creating enforceable remedies in relation to breach of public register privacy principles - recommendation 95;
- providing for suppression of information on public registers for reasons of personal safety or harassment - recommendations 97, 98, 99;
- enabling certain jurisdictional matters to be taken by a complainant to the Complaints Review Tribunal - recommendation 105;
- criminalising the knowing destruction of documents in order to evade an actual access request - recommendation 149;
- outlawing coerced access requests - recommendations 151, 152.

I do not consider that these changes will entail any significant compliance costs.

Effectiveness of Office of the Privacy Commissioner

The Privacy Commissioner established by the Act is given a number of tasks. The Act grants various powers to enable those tasks to be effectively performed. I have considered whether the provisions of the Act are adequate, or can be improved, to ensure that my Office is able to perform effectively. For the most part I believe that the provisions in the Act are satisfactory. Nonetheless, I have identified a number of areas where potential effectiveness will be enhanced by amendment to the Act.

Relevant recommendations include:

- enhancing powers to address privacy issues by codes of practice - recommendations 18, 74;
- excluding the official information statutes from determining questions of release of information from public registers - recommendation 100;
- clarifying requirements concerning action on receipt of complaints - recommendation 104;
- establishing a process for referring jurisdictional questions to the Complaints Review Tribunal - recommendation 105;
- establishing a formal power to defer complaints - recommendation 106;
- seeking adequate funding so that complaints may be processed with due expedition - recommendation 108;
- enabling the enforcement of assurances - recommendation 112;
- enabling requirements to be complied with within an abbreviated time period - recommendation 114;
- varying the information matching guidelines to require examination of a proposed programme's compliance with Part X - recommendation 124;
- requiring periodic review of information matching agreements - recommendation 125;
- funding information matching monitoring activities by the agencies undertaking matching - recommendation 132;
- extending the limitation period for offences under the Act - recommendation 150.

Interaction with other laws

The Privacy Act is obviously not the only law bearing upon the handling of personal information. These include, amongst others, laws concerning:

- obtaining information - such as the statutory powers of the DSW to obtain information and documents from individuals and businesses;
- holding or retaining information - such as the Archives Act and requirements in tax laws requiring the retention of financial records;
- disclosing information - such as the secrecy provisions applied to certain government agencies prohibiting the disclosure of information;
- accessing information - such as the public register provisions and the Official Information Act.

The Act currently spells out how it is to relate to other pieces of legislation. Generally it provides that the information privacy principles are subordinate to provisions in most other enactments.

I have considered whether the way the Act currently deals with the interaction of other laws is satisfactory. One of the main problems that I have attempted to address concerns the lack of awareness by some users of the Act of the provision saving the effect of other laws. Amongst other things, my recommendations seek to make the interrelationship plainer so as to reduce misunderstanding. The term “savings” is a technical legal term which is not readily understood by lay readers of the Act. Some would appear to be unaware that the privacy principles do not override other laws.

Relevant recommendations include:

- changing the marginal notes to the savings provision in section 7 to direct users of the Act more clearly to its relevance - recommendation 2;
- moving material relating to the saving of the effect of other laws into the various principles as new exceptions - recommendations 30, 31(a), 33;
- relocating the provisions saving the withholding effect of other laws into Part IV as a reason to withhold information - recommendation 32;
- refashioning the savings provision concerning enactments imposing more restrictive obligations of non-disclosure - recommendation 33;
- providing for the expiry of the saving of regulations allowing for refusal of access requests - recommendation 34;
- clarifying the relationship between the principles and public register provisions - rec-

- recommendations 92-95;
- bringing provisions in other statutes into the public register regimes of the Privacy Act and Domestic Violence Act - recommendations 96 and 97;
- excluding the official information statutes from questions of release of information from public registers - recommendation 100;
- tidying up the provisions concerning the transfer of complaints between, and consultation with, the Privacy Commissioner and other statutory complaints bodies - recommendations 102, 107, 145 and 146.

Compliance and administration costs

Business compliance cost reduction has been an issue for government in recent years. Indeed, the matter has been a central feature leading to the present design of the Act. Most notable is the absence of a registration or licensing system which is the norm in Europe. The Privacy Act adopts an outcomes-oriented approach whereby the Act prescribes the standards but agencies have a great deal of flexibility in the way that they may comply with them. In my review I examined various features which contribute to the low compliance costs imposed by the Act and examined whether it would be possible through amendment to the Act to improve the position even further with respect to compliance costs.

Compliance costs revolve around the costs borne by agencies in complying with the requirements of the Act. It should not be assumed that, in the absence of an Act, there would be an absence of costs associated with meeting privacy risks and issues. Where statutes do not broadly cover privacy issues a variety of sectoral laws is normally combined with voluntary self regulation and laws relating to confidentiality. All these involve compliance costs. Costs borne by agencies cannot be considered in isolation from the costs imposed upon individuals in exercising their rights and entitlements under the Act. Accordingly, I also examined the regime established by the Act in that regard particularly with respect to charges that individuals may have to pay in order to have access to information or to seek to have it corrected.

Frequently issues of compliance costs interrelate with the administration costs of agencies established by a law. I am of the opinion that the work that my office does or might undertake in relation to education and publicity, particularly in offering compliance advice, contributes to minimisation of compliance costs among agencies. There are severe restrictions upon what I can attempt on my present budget given the need to apply resources to a significant complaints backlog. A 12 month queue before complaints are investigated is not only unfair to the complainants, and may undermine the credibility of the processes established, but also increases costs of the respondent agencies. In particular, where there is a continuing relationship between an individual and an agency, whether as customer, employee or otherwise, there is a great deal to be said for being able to promptly tackle the complaint through the Act's conciliatory processes which frequently lead to settlements which may often enable the relationship to continue. A delay in commencing the investigation also means that the events are not so fresh in people's minds leading to inefficiencies and problems in the investigation process and potential problems for the agency establishing its position, and may permanently sour the relationship.

In respect of the problem of administration costs, I believe that the solution is primarily to be found in the application of appropriate funding to meet the level of complaints being processed. Nonetheless, I have examined the provisions of the Act to see whether any amendments are desirable to ameliorate the problems. The recommendations I have made will contribute to the current low costs of compliance and help to prevent rises in costs in the future. I have considered requiring applicants to meet some costs of processing certain applications and giving me more statutory discretion to defer investigating complaints where it is reasonable that the individual first pursues an alternative.

A number of recommendations would improve ease of use of the Act. They also have an objective of reducing compliance costs.



Recommendations include:

- limiting information privacy principle 12(2) solely to the reassignment of unique identifiers originally generated, created or assigned by a public sector agency - recommendation 28;
- adopting a transborder data flow provision designed to have the least compliance cost effect on business - recommendation 35(a);
- repealing provisions for the preparation of a nationwide directory of personal information or, if provision for a directory is retained, requiring the Commissioner to have regard to compliance costs when determining whether or not to prepare a directory - recommendations 40, 42;
- permitting agencies to choose a privacy officer who is not within that agency - recommendation 44;
- entitling public sector agencies to make a reasonable charge for making information available to a foreigner who makes the request from overseas - recommendation 62;
- allowing exemptions to be obtained from having to deal with an individual's access request for a period where it can be shown that the individual has lodged requests of a repetitious or systematic nature which would unreasonably interfere with the operation of the agency and amount to an abuse of the right of access - recommendation 66;
- allowing exemptions to be obtained in relation to principle 9 (retention of information) - recommendation 79;
- enabling liability to be shared between an agency and individual where that individual, in a domestic or household capacity, misleads the agency into wrongly disclosing information - recommendation 82;
- enabling all charging complaints to be dealt with by the Privacy Commissioner without the prospect of further Tribunal proceedings - recommendation 110;
- integrating local government delegation provisions into a more convenient statutory location - recommendation 147.

Recommendations relevant to the administration costs of my office include:

- providing for the Commissioner to put a funding case directly to Treasury and relevant Ministers - recommendation 37;
- repealing provision for the Commissioner to publish a directory of personal information or alternatively transferring the function to the Ministry of Justice - recommendations 40 and 41;
- empowering the Commissioner to require a representative body to undertake public notification of an application for a code - recommendation 77;
- empowering the Commissioner to require an applicant for a section 54 exemption to publicly notify the application - recommendation 80;
- enabling the Commissioner formally to defer certain types of complaints - recommendation 106;
- funding the office so that complaints can be processed with due expedition - recommendation 108.

Ease of use of the Act

In many cases, I am satisfied that the substantive law bearing on an issue is appropriate and yet some people have found provisions difficult to follow. My suggestions will help to achieve the law's objectives through better agency compliance and better understanding of the rights of individuals.

My recommendations try to avoid substantial rewriting. This is to retain the benefits of familiarity gained by those using the Act over the last few years. So I have taken a minimalist approach which may deceive the reader into thinking that the changes are inconsequential. I am confident they have the potential to improve the Act's "user-friendliness" and thus avoid the chance of misinterpretation.

Some recommendations are:

- implementing changes in legislative drafting styles adopted by the Parliamentary Counsel Office and arranging a full reprint - recommendations 1, 4;

- making marginal notes and headings more informative - recommendations 2, 133;
- providing more useful comparative notes to equivalent provisions in the official information legislation - recommendation 3;
- altering definitions - recommendations 13, 14, 15, 50, 117-121, 137;
- replacing complex provisions with clearer provisions - recommendations 17, 64, 154;
- using the phrase “purpose or purposes” in the principles - recommendation 19;
- simplifying the provisions relating to the impact of other laws and relocating them to where users would expect to find the content - recommendations 30-33;
- simplifying the layout, and clarifying the content, of the withholding grounds - recommendations 47, 48, 52, 57, 58;
- amalgamating sections and relocating some material into schedules - recommendations 107, 145, 147;
- rewriting aspects of the information matching controls - recommendations 130, 135, 136, 137;
- removing spent or unnecessary provisions - recommendations 70, 102, 153.

“Adequate protection” in terms of the EU Directive

The EU Directive on Data Protection is required to be implemented in EU countries by October this year. The EU Directive will oblige member states to restrict the transfer of personal data to third countries if that data will not be subject to “adequate protection”. The existence of the Privacy Act is the best guarantee that the Europeans will accept that data on Europeans will be protected when transmitted to New Zealand. Generally speaking, New Zealand’s Privacy Act is perceived by most commentators as one of the best in the world outside Europe. Indeed, the protection that it offers to personal information is superior to that offered in many European jurisdictions, particularly in respect of information which is not “automatically processed”.

Nonetheless, I have carefully scrutinised the Act to be sure that its provisions will be judged by European standards to be “adequate”. To be adequate our law does not need to have identical provisions to the EU Directive. It is believed that the law will largely be judged in its totality. Our Act should, in general terms, pass such an adequacy test with flying colours.

However, there are two aspects which somewhat cloud this rosy picture. New Zealand’s law is in danger of failing an adequacy test in so far as it denies access rights to foreigners except when they are actually in New Zealand. This would effectively deny most Europeans one of the key data protection entitlements in any law. In my view, that should be put right as soon as possible.

The Office of the Privacy Commissioner, with its complaints jurisdiction, provides the independent national institution that is a central feature of an adequate system for the protection of privacy in European eyes. I have no doubt that the basic legislative arrangements for the Privacy Commissioner would be a feature which supports an adequacy case in European eyes. However, the underfunding of my office, which has led to complaints waiting in a 12-month queue, may cause EU Commissioners to question the adequacy of a central feature of our Act. An investigation delayed for that long can lose credibility as a compliance mechanism. It is important in this context, in my view, that this central aspect be put right.

Another issue relates to the possibility of European agencies diverting data transmissions through New Zealand to another country so as to circumvent the EU prohibition. This also should be put right.

Amongst my recommendations is one concerning the deletion of details from mailing lists which is modelled upon provisions in the EU Directive. Its current absence in our law is not likely to call into question the adequacy of New Zealand’s laws. Rather, the EU Directive provides a very promising model to copy from in according appropriate protection to the privacy of New Zealanders’ personal information.



Reference may be made to the recommendations:

- providing for the deletion or blocking of personal information held by an agency for direct marketing purposes - recommendation 25;
- providing a mechanism to enable mutual assistance to be extended to prohibit transborder data flows in circumstances where New Zealand is being used as a conduit for transfers designed to circumvent controls in EU and other privacy laws - recommendation 35(a);
- abolishing the standing requirements for foreigners to exercise access rights - recommendation 61;
- seeking that adequate funding should be made available so that the volume of complaints can be processed with due expedition - recommendation 108.

PRIVACY AT THE END OF THE TWENTIETH CENTURY

As we approach the dawn of the new millennium the Privacy Act provides a sound framework for addressing a range of privacy issues. Nonetheless, the appropriate protection of privacy necessarily is an ongoing process of refinement, evaluation, experimentation and consolidation. Technology will not remain static to suit a legal rule. Nor do the demands or expectations of the international community or New Zealanders. Already, I have identified issues which deserve further study and which may, at a future point, warrant amendment to the law.

The information privacy principles are based upon the 1980 OECD Guidelines. These represent a culmination of 1970s thinking on information privacy issues. Many experts believe that the OECD Guidelines have stood the test of time well and continue to be adequate to the task. However, from the early 1990s the OECD Guidelines have been subject to criticism from several quarters.¹ It has been suggested that they are not as technologically-neutral as first supposed with some key concepts, such as “data controller”, based upon understandings of existing information storage media, such as main-frame computers, rather than distributed computer networks or the Internet.

The OECD has seen scope for new principles. Its Guidelines on the Security of Information Systems (1992) and Guidelines on Encryption Policy (1997) each contained further principles relevant to information privacy. Guidelines are in preparation in relation to consumer protection in electronic commerce.

Other international bodies, such as the EU, Council of Europe and the ILO, to name but three, have also been involved in more specific standard setting in relation to information privacy issues. There has been concern to ensure that principles are up to the challenge of the “Information Society”.

In my review I have examined the laws of other countries and developing general international guidelines relevant to the better protection of individual privacy. As a result I have sometimes recommended the adoption of new provisions in our Act. A principal example is recommendation 25 in which I propose that individuals be entitled, as in the EU Directive on Data Protection, to have their names removed from direct marketing lists.

One of the discussion papers canvassed the possibility of new privacy protections and mentioned a number of the new principles being developed elsewhere. Twenty-seven submissions were received. In this report I have stopped short of recommending the adoption of the innovative principles mentioned in that paper. This is not because I believe that they are misconceived or of little importance. A number of new principles that have been proposed, such as those guaranteeing anonymity, promise to protect privacy better in some situations than our existing principles.

Some of the more novel ideas require more study than has been possible, or appropriate, in this review. Others may be more amenable to study when they have been fully imple-

¹ See, for example, John Gaudin, “The OECD Privacy Principles - Can They Survive Technological Change?” (1997) 3 *Privacy & Policy Reporter* 143 and 196.

mented in their own jurisdictions. For example, the Australian National Principles for the Fair Handling of Personal Information (February 1998) have been released on the understanding that they will be reviewed in 6 to 12 months time.

It is an active time for the development of privacy protections internationally. Amongst other developments to follow in the next couple of years are the:

- completion of national implementation of the EU Directive in Europe;
- initiatives in the USA involving enhanced self regulation and sectoral legislation;
- extension of privacy protection to the private sector in Canada;
- review of the wave of new privacy laws enacted between 1992 and 1997;
- conclusion of the international debate about access to encryption technology;
- implementation in Australia of the recent National Privacy Principles;
- International Standards Organisation's work directed towards establishing processes for certifying business compliance with privacy standards;
- development of privacy enhancing technologies enabling anonymous consumer transactions.

This is only a small list of what is happening internationally in respect of new privacy protections. There are a wide variety of ideas which have been advanced for taking the protection of privacy beyond the well trodden route of data protection principles found in the OECD Guidelines. A promising local example is the National Principles for the Fair Handling of Personal Information which has derived principles from the groundbreaking Australian Privacy Charter (1994). For example one principle, directed to a matter not currently addressed, is:

If we can (and you want to) we will deal with you anonymously

Wherever it is lawful and practicable, individuals should have the option of not identifying themselves when entering transactions.

Another novel principle, found in the Australian Privacy Charter, states:

“No disadvantage

People should not have to pay in order to exercise their rights of privacy described in this Charter (subject to any justifiable exceptions) nor be denied goods or services or offered to them on a less preferential basis. The provision of reasonable facilities for the exercise of privacy rights should be a normal operating cost.”

Another principle without precedent is under consideration in the context of the Human Genome Project and other initiatives involving genetic technology. People studying the issues are beginning to speculate whether notions of privacy, dignity and personal autonomy need to be strengthened by a “right *not* to know personal information” in certain circumstances. For instance, if one family member seeks a genetic test which reveals the probability of a debilitating condition should other family members be informed? Many individuals prefer to live their lives without any inkling of the probabilities of what the future holds for them. As genetic technology is further developed society may need to develop principles concerning the handling of such personal information which go beyond those in the OECD Guidelines of 1980.

Clearly there is much work to be done and challenges faced in the coming years. My confidence that the Privacy Act is soundly based, and works well in operation, should not be mistaken for complacency about the challenges to the protection of privacy. There are many chapters yet to be written in the report on our society's response to privacy issues but these will need to await further specialist examinations and the next periodic review of the Privacy Act.



