



Privacy Commissioner
Te Mana Matapono Matatapu

DP 9

REVIEW OF THE PRIVACY ACT 1993
DISCUSSION PAPER No. 9

COMPLIANCE AND ADMINISTRATION COSTS

The Privacy Commissioner is reviewing the operation of the Privacy Act under section 26 of the Act. The Commissioner will consider whether any amendments to the Act are necessary or desirable and will report his findings to the Minister of Justice.

This paper is one in a series which will cover the entire scope of the Act and highlight some issues. To find out which other discussion papers have been released, and to obtain copies of them, you may contact the Commissioner's office. Copies of the discussion papers will also be available through the Commissioner's web site.

The Privacy Commissioner welcomes comments on this paper and seeks responses to any specific questions raised. Submissions should be made in writing and be forwarded to the Commissioner's office by post or email no later than **10 November 1997**.

The Commissioner will hold a series of consultation meetings in the main centres and some regional cities during November. If you would like to be invited to a consultation meeting please indicate this with your written submission.

Contact details for consultation

Privacy Act Review 1997
Office of the Privacy Commissioner
P O Box 10-094
Wellington

fax: 04-474 7595 privacy hotline: 0800-803 909 email: privacy@actrix.gen.nz

For general enquiries about the review please speak to the Enquiries Officers at the freephone number. If you have a more detailed enquiry concerning your submission or the review please speak to the Codes and Legislation Officer at 04-474 7597.

Background materials on the Privacy Act available on the Internet at:
<http://www.knowledge-basket.co.nz/privacy/welcome.htm>

ISBN 0-478-10364-6 September 1997

CONTENTS

		Page
1	INTRODUCTION	3
2	BACKGROUND	4
	International context	4
3	COMPLIANCE AND ADMINISTRATION COSTS	5
	Definition of compliance costs	5
	Excessive compliance costs	5
	Administration costs	5
4	THE PRIVACY ACT	8
	Development	8
	Design	8
	<i>Comprehensive coverage</i>	8
	<i>Broad principles</i>	9
	<i>Flexible mechanisms</i>	9
	<i>Choice in how to comply</i>	10
	<i>Independent Privacy Commissioner</i>	10
	Implementation	11
	Types or sources of costs	12
	Compliance cost implications	12
5	SPECIFIC ISSUES	14
	Layout and wording of Act	15
	Access requests	15
	Complaints	16
	Privacy officers	16
	Advance rulings	17
	Specific exemptions	18

1 INTRODUCTION

This paper looks at compliance costs incurred by agencies in regard to the obligations of the Privacy Act. It also looks at the administration costs of the Office of the Privacy Commissioner, where the work of that office might contribute to reducing the compliance costs of agencies. The paper examines compliance and administration costs at two levels:

- the design or scheme of the Act generally;
- specific features and provisions.

Compliance costs in regard to obligations imposed by legislation are a current issue for government. Costs (if any) associated with complying with the Privacy Act are believed to be modest for most agencies.¹ The paper solicits information about such costs and suggestions to reduce them and it is thereby hoped that ideas coming out of the review may help ensure that these costs remain modest, and perhaps even be reduced, while ensuring that the fundamental principles underlying the Act are not undermined.

It is understood that most equivalent laws in overseas jurisdictions impose more compliance costs than our model. The New Zealand Privacy Act has a number of features conducive to minimising such costs, by providing certainty yet allowing flexibility, giving scope for choice in implementation, and establishing low-cost and effective complaints resolution which avoid the courts. The review is the opportunity to build on the best features of our privacy law.

This paper includes general questions about compliance and administration costs, seeks feedback from respondents' own experience, and identifies provisions in the Act that are relevant to the topic.

¹ Although, as might be expected, the implications of the Act may be somewhat greater for agencies whose business is largely based upon the use of personal information. Even in those cases it is believed that after the implementation of initial changes required by the Act the on-going costs remain modest.

BACKGROUND

Compliance costs cannot be looked at in isolation. Trade-offs are involved. Changes designed to address compliance costs need to be considered in the light of the effects on the objectives of privacy law and the effects elsewhere, say, the costs to government or to individuals (such as customers or employees). Care must also be taken that the outcome of moves to reduce compliance costs do not result in a reduction in compliance with the objectives of the Act rather than in the costs of complying with them.

In addition to the traditional concern with the relationship between the state and the individual in protecting privacy as a human right, privacy is a global consumer issue, in particular with new technologies. Privacy protections are therefore being driven at the individual and consumer level, as well as by the needs of states, and international commerce, in the overall context of the developing global information society.

International context

New Zealand implemented OECD guidelines, earlier accepted, through the Privacy Act.² A significant feature of these guidelines is an attempt to ensure member countries have consistent minimum privacy laws so that international trade is not impeded. More recently the prospect of scrutiny of countries' privacy law has arisen pursuant to the 1995 EU Data Protection Directive.³ This generally prohibits EU member countries from transferring personal data to non-EU countries unless "adequate" privacy measures are in place. This directive has acted as a spur for various jurisdictions to consider whether they should enhance their privacy legislation. For instance Hong Kong, much concerned for its business sector and heavily dependent upon international trade, was spurred to adopt a privacy law covering public and private sectors.

New Zealand's Privacy Act is presently "adequate" in EU terms and we need to ensure that any changes do not jeopardise that position. Some other countries do not have that certainty in their business environment. Indeed, New Zealand presently has a competitive advantage over other jurisdictions in the region in regard to such international requirements. The state of Victoria, for example, is thought to be intending to legislate for information privacy for just this reason, given a government commitment to foster electronic commerce.

² OECD, *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, 1980 ("The OECD Guidelines"). These, and the EU Directive mentioned below, are available in Butterworths, *Privacy Law and Practice*, Wellington, 1993-97.

³ EU, *Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, Article 25, 24 October 1995 ("The EU Data Protection Directive"). Transborder data flow controls also exist in the laws of Quebec, Taiwan and Hong Kong.

COMPLIANCE AND ADMINISTRATION COSTS

Definition of compliance costs

There is no statutory definition of "compliance costs". The Ministry of Commerce defines them as:

"the costs to affected parties of interacting with government in meeting an obligation or obtaining a service."⁴

Much of what it costs business to meet requirements of the Privacy Act would not fit within this definition. In fact, under this definition the Privacy Act arguably imposes no compliance costs. However, others take a rather wider view of the costs of complying with statutory obligations.

The Ministry distinguishes compliance costs from other costs by stating that compliance costs are incidental to the obligation itself and are often related to the providing of information to the government. Examples given include: costs of understanding the obligations; form filling costs; time taken in maintaining records or registers; anxiety costs caused by complex requirements; time spent determining how an obligation relates to a party; and the resources required to translate a complicated requirement or regulation into the actions a party is obliged to carry out.

Perhaps as an alternative to the Ministry's approach one could look at compliance costs in terms of:

- what extra things the Act requires agencies to do;
- what things agencies might like to do which the Act now prohibits;
- what things agencies do which the Act makes them do differently.

Q1 What are compliance costs? On what should the Privacy Commissioner concentrate in looking at the issue of such costs?

Excessive compliance costs

Compliance costs might be thought "excessive" where it would be practicable to achieve the essential objectives of a piece of legislation without all or part of the costs actually encountered.

"There are numerous causes of excessive compliance costs. Most originate from the measures themselves, their design and how they are administered, but others arise from difficulties which smaller and newer firms, in particular, have in managing their obligations."⁵

The causes of excessive costs have been suggested to include:

- insufficient consideration of compliance costs in policy development;
- excessive complexity of regulations, processes and forms;
- failure to tailor compliance requirements to different types of business;

⁴ Ministry of Commerce, *Compliance Cost Assessments and Statements: Guidelines for Departments*, January 1997, page 7.

⁵ Ministry of Commerce, *op cit*, page 5.

- lack of regular monitoring and review of the continuing need by government organisations for specific information requirements obtained by the private sector;
- insufficient explanation of the rationale for an obligation (firms find it easier to comply if they know what the information that they supply will be used for);
- lack of information about what a measure means for individual companies (this is particularly relevant to new complex pieces of legislation); and
- for individual businesses themselves, a lack of the management systems and skills necessary to comply, due to factors such as lack of experience, capabilities or equipment.⁶

As will be seen, the Privacy Act, in its design and administration directly addresses many of these matters. Indeed, in some of these respects it may be seen as a model in compliance cost minimisation. Agencies' experiences in this regard are welcomed.

Q2. Are there any aspects of the Privacy Act which fall into any of these categories of causes of excessive compliance costs?

Excessive compliance costs can have the following negative effects:

- *discourage growth and employment* - they divert the energies and resources from more productive uses, deflecting firms' focus from core business;
- *erode international competitiveness* - which will be the case if firms offshore face lower compliance costs; and
- *hinder compliance* - if compliance costs are too burdensome, businesses are less likely to meet their obligations.⁷

The handling of information, including personal information, is part of the core business of many agencies and the information privacy principles, which lie at the heart of the Privacy Act, are conducive to good information handling. The Act compares favourably in terms of compliance costs with overseas privacy provisions and in fact aids our international competitiveness by passing EU and other "adequacy" scrutiny to receive data from Europe and elsewhere. Minimisation of compliance costs was a major design factor in the choice of model adopted. Thus the Act gives agencies maximum choice over how they meet its obligations, and incorporates features such as codes of practice, which allows the obligations to be tailored to the circumstances of particular agencies or sectors. Indeed, in a report on business licences and regulation reform, the Australian Bureau of Industry Economics said that:

"Of the data protection arrangements in use in the jurisdictions examined ... the New Zealand approach may provide the most cost-effective and flexible approach. It avoids the compliance and administration costs associated with a licensing scheme such as that used in the United Kingdom. Its consultative nature is likely to encourage compliance and it is capable of accommodating differences in circumstances across industries, professions or business."⁸

⁶ Minister of Finance, *Business Compliance Cost Reduction: A Government Policy and Discussion Paper*, Wellington, December 1994, page 6.

⁷ Ibid, page 7.

⁸ Bureau of Industry Economics, *Business Licences and Regulation Reform*, June 1996, page 53.

Governments recognise that properly designed and administered regulation can improve economic performance, enhance social benefits, accommodate technical innovations, respond to consumer needs and increase opportunities for trade and investment.

Administration costs

Administration costs are the costs to a government agency in administering an obligation or regulation, funded by taxation or user charges. This includes the cost of development, compliance, and complaints investigation and adjudication. In some instances decisions can be taken to transfer compliance costs from the private sector to government as administration costs or vice versa.

The following example demonstrates a split between compliance and administration costs. A government department wants certain information which is held by various entities in the private sector. It may send out one thousand demands to banks, employees and landlords using statutory powers to require the furnishing of that information. Suppose that it costs \$10 for each agency to assemble relevant data and prepare an answer. The department could reimburse the agencies, which would show up as an administrative cost and come out of its budget, or it can rely on its powers and leave costs where they fall as a compliance cost. Different incentives exist to reduce or impose both types of costs.

The Privacy Act is administered by the Ministry of Justice. A number of statutory functions are conferred on the independent Privacy Commissioner. Receiving and investigating complaints form a major part of the Privacy Commissioner's work. Last year he received 1200 complaints. Apart from receiving complaints and enquiries, his functions include, for instance, the ability to inquire into any privacy matter, issue codes of practice, carry out publicity and education, and examine proposed legislation to consider its effect on privacy.⁹

⁹ Most of the Commissioner's functions and powers are set out in section 13 of the Act.

THE PRIVACY ACT

Development

The Privacy Act provides a relatively "lightheaded" approach to protecting privacy and compliance costs were explicitly taken into account when considering options for its design.¹⁰ Many options were explicitly rejected because of the greater compliance costs they would impose.

In addition, extensive changes were made by the Select Committee during an 18-month examination of the bill, many of which were designed to minimise the compliance costs to business. Changes in this regard included:

- providing the mechanism of codes of practice, rather than more limited and burdensome exemptions requiring approval by the Complaints Review Tribunal;
- provision for one-off exemptions to be granted by the Commissioner;
- excluding some organisations and information from coverage by the Act while generally maintaining a seamless application to the public and private sectors;
- providing for transitional provisions which eased implementation in the first 3 years;
- redrafting some of the privacy principles to make them more workable and flexible;
- modifying the standard imposed in some principles by reference to what an agency "believes on reasonable grounds" or what is "reasonable in the circumstances";
- allowing the private sector to charge for access requests.

Design

The Privacy Act has the following design features which, among other considerations, are beneficial to reducing compliance costs. It provides:

- comprehensive coverage in terms of both agencies and type of information;
- clear broad principles with appropriate exceptions;
- flexibility to tailor requirements to the specific needs of industries or agencies;
- choice in how to comply - no registration, licensing, notification or prescribed forms;
- an independent Privacy Commissioner whose functions include investigating complaints, education, advice and policy.

Comprehensive coverage

The Privacy Act controls how personal information is handled by agencies in all sectors, ranging from collection through storage, use and disclosure. It provides individual access and correction rights. It covers all personal information with the same set of rules regardless of the form in which information is held (manual or electronic). This provides for clarity, certainty and coherence of privacy obligations.

Hong Kong's new 1995 Personal Data (Privacy) Ordinance also covers both the public and private sectors as do most European laws. In contrast, Canada and Australia mainly cover

¹⁰ See McBride, *Data Privacy: An Options Paper*, 1987, a report commissioned by the Minister of Justice. The report examined a number of existing schemes including licensing, registration, legislation covering particular sectoral data handling activities. Compliance and administration costs were key aspects of the consideration.

the public sector.¹¹ Canada has committed to legislating to cover its private sector by the year 2000. The New Zealand Act has been cited as a possible model.

Australia has had to amend its privacy law to cover a growing number of private sector areas, such as credit reporting, tax file numbers, and some outsourcing to address specific needs or problems. Existing law is something of a patchwork with resultant complexity. Plans to cover the private sector along the lines of the New Zealand model have been halted at federal level leaving some uncertainty as to future handling of privacy matters (with speculation that some individual states may act). In Australia there is a natural wish to have a uniform approach rather than inconsistent federal and state sectoral legislation. Uncertainty can impose costs on business, especially as the implications of EU requirements are considered - an uncertainty New Zealand does not face.

Coverage of both private and public sectors is consistent with other modern New Zealand law and perhaps acknowledges in part the changes to the public sector over the last decade, with privatisation, contracting out and outsourcing of formerly government-provided functions. In information terms, no boundary is recognised in the flow of data between the public and private sectors. Seamless law has a variety of benefits by avoiding lacunae, loopholes and demarcation disputes. A further benefit is the transferability of people, experience and techniques between the public and private sectors having the same privacy requirements.¹² It is also consistent with notions of the "level playing field" and maximum choice in provision of services.

In terms of comprehensive coverage of all types of information New Zealand compares favourably with the United Kingdom whose Data Protection Act 1984 regulates the use, quality and protection of automatically processed information only. Nearly all modern privacy laws have dropped the distinction between automatically processed and manual data, as will European countries when the EU Directive is implemented.

Broad principles

The information privacy principles, as the core of the Act, provide a set of clear and comprehensive principles, drawn from the OECD Guidelines, with specific exceptions provided for to provide flexibility to cater to individual circumstances where it would be inappropriate or too difficult for the Act or the principles to apply.

Flexible mechanisms

The Act has a number of mechanisms providing for flexible application of privacy obligations.

Of most importance is the provision for codes of practice tailored to the specific needs and practices of different agencies, industries or professions, activities or information. Usually professional or industry bodies draw up early drafts of codes, although the Commissioner may initiate the process. Such mechanism aids interpretation as well as "ownership" of

¹¹ The Quebec law covers the private sector.

¹² By contrast there has been some frustration at the unfamiliarity with Official Information Act requirements and ethos of some private sector personnel brought into the public sector.

the legislation's obligations, thus reducing the costs of, while at the same fostering, compliance. In fact, few codes of practice have been needed with most industries being able to operate within the principles. Those industries which were initially most concerned with the application of the Privacy Act to them, such as banking, insurance and direct marketing, have found that, in fact, they can readily live within it.

There are also specific authorisation procedures in appropriate individual cases (section 54).

The operation of the information privacy principles can be overridden by other enactments (see section 7), which gives the public sector the ability to modify the application of the privacy principles to their activities and those aspects of the private sector regulated by statute (e.g. the health sector).

Choice in how to comply

The Privacy Act provides maximum choice in how agencies comply with the Act suited to their own business. Agencies can establish their own policies consistent with the principles and, broadly speaking, as long as they are open about them they can broaden or narrow the purposes for which personal information can be used or disclosed.

There are no licensing, registration, or notification requirements, or prescribed forms as in many other jurisdictions. For example, in the United Kingdom all agencies operating a computer system containing personal data must register and pay a fee. The compliance and administration costs incurred in registering, as well as the complexity of the regime, were criticised by the UK Deregulation Task Force in 1995.¹³

The Australia requirement for annual returns to be made by all federal agencies covered, has been the subject of similar criticism.¹⁴

Independent Privacy Commissioner

The Privacy Commissioner in his various functions has a duty to have regard to, amongst other matters, the rights of government and business to achieve their objectives in an efficient way (section 14). Accordingly, he will at times expressly consider compliance costs as an interest competing with privacy.

The complaints role conferred by the Act on the Commissioner provides for a relatively timely, low-cost resolution of complaints, with an emphasis on seeking a resolution and eschewing punishment.¹⁵ It may be thought of as an example of restorative justice. Cases which have not settled may be taken to the Complaints Review Tribunal. Only 30 cases have found their way to the Tribunal out of 2500 complaints completed to date.¹⁶ This provides a less costly approach for parties and for the state than the traditional litigation model and has previously been successfully used in discrimination and sexual harassment

¹³ In *Business Licences and Regulation Reform*, page 50.

¹⁴ See Privacy Act 1988, section 14, information privacy principle 5(4)(b).

¹⁵ In contrast to the privacy laws of many countries which are enforced through criminal sanctions.

¹⁶ However, note that not all complaints arising from mid 1993-1996 could be referred to the tribunal because of transitional arrangements.

complaints. It carries less direct cost to industry than having to provide their own individual dispute resolution mechanisms (such as an industry ombudsman). Whilst it allows individuals to pursue grievances without either the expense or delays of litigation, it also means that small businesses are not held to ransom by wealthy individuals bringing court proceedings beyond the ability of the business to defend.

There are many hundreds of thousands of agencies and most never have a complaint made against them. The Privacy Commissioner regards the complaints process, beyond the resolution of particular complaints, as enabling the identification of issues agencies need to face. Changing agencies' practices avoids future complaints, and assurances of such change are a frequent component of settlement agreements.

Definitive interpretations of some aspects of the Privacy Act may need to await Tribunal cases. As most of the principles did not become fully enforceable until July 1996 it will be a few years yet before a wealth of precedents is built up. After a while the task of advising agencies on the law may become more straightforward. In the meantime the Privacy Commissioner has issued many case notes as to the approach he has taken to interpreting the principles on real complaints. The Privacy Commissioner provides fact sheets, an 0800 enquiries number, case notes, and a web site all free of charge. He also provides compilations of explanatory materials and puts on training workshops at modest cost-recovery charge. The Privacy Commissioner has considered such initiatives as important to assist agency compliance. However, there is limited ability to provide advice to agencies on specific proposals with privacy implications, both for resource reasons and because of the possibility of conflict with complaints resolution responsibilities.

This review, and future reviews required under the Act every five years, are another positive feature in regard to reconsidering and minimising compliance costs.¹⁷

Q3. What more could the Privacy Commissioner do within his budget to reduce compliance costs? What else could be done to minimise compliance costs, in particular for smaller businesses?

Implementation

There are initial compliance costs in understanding and implementing new legislative obligations. The Act therefore provided transitional arrangements.¹⁸ These were that existing forms and marketing lists could be used for a period, and that the full effect/remedies of the information privacy principles were phased in over three years, thus moderating the initial impact. During this period the Commissioner, amongst other things, prepared materials to assist agencies, such as fact sheets and case notes, and assigned and trained 3 staff to answer enquiries from agencies and the public on a toll free number and by mail.

It might be expected that these initial implementation costs would be much reduced now, although other costs will continue or even increase with greater awareness by individuals of their rights. Agency staff should now be familiar with the Privacy Act requirements and

¹⁷ Privacy Act, section 26.

¹⁸ See Privacy Act, sections 9 and 79.

the level of understanding should be improving. It might therefore be expected that routine compliance aspects might now be handled more cheaply and quickly. However the experience in other jurisdictions is that with a more sophisticated understanding of the law comes the application of the principles to more complex situations and "pushing the boundaries" in both complaints and in the application of new technology.

Types or sources of costs

Most agencies deal with, at least, personal information about their employees. Others also collect or hold information about customers or clients. The collection, holding, use or disclosure of this information is subject to the information privacy principles.

Costs related to the Privacy Act involve the appointment of privacy officers, review of forms, instituting complaints mechanisms, dealing with access requests, and initial education and training. Some of these costs are moderate and would have been essential for any new law, in particular one of such relevance to employers or business, regardless of how well it caters for compliance costs. Some may be characterised as "one-off" costs incurred largely at the commencement of the Privacy Act; others are ongoing, although perhaps to a lesser degree than initially. In some cases agencies say they would have costs for training staff to comply with the terms of their fiduciary relationships with customers and the law of confidence. Banking and insurance sectors have always had to employ highly trained staff and security and similar issues are prominent in training.

Q4. What actual business costs are involved in complying with the Privacy Act?

Compliance cost implications

The Act establishes a set of principles which are clear, but flexible in application. There is no base level of costs and there may be no costs at all for some agencies. There are no direct compliance costs in registration or licensing paperwork and no fees, as is required in other jurisdictions or legislation. It is up to agencies to devise their own procedures and forms, giving them maximum choice in how to comply with the principles. Although there is a cost in changing information policies, agencies will usually need to have and revise such policies, formally or informally, in any case.

Since the information privacy principles may be said to be based on good or fair administrative practice, any costs in changing practices to meet their requirements should also produce long term administrative benefits. Comments made to the Commissioner's office have often included that existing good management practices and policies were already in accordance with the Act; that its introduction was seen as a positive step and led to better file management; that it has made staff more professional; that there have been no significant costs associated with it; and that the merits far outweigh the costs.

There will always be costs in collecting, storing and providing information. Adherence to sound information handling practices is also good business. If the Act did not provide guidelines then businesses, professions and others might have needed to devise something similar. This is particularly true for "information rich" industries whose business involves personal information to a significant extent, such as credit reporting, healthcare, banking

and insurance. Indeed, some of these sectors already catered to this need with their own rules about confidentiality and rights of access (although not always to the satisfaction of individuals).

In terms of the factors causing excessive compliance costs outlined earlier in the paper:

- *Insufficient weight being given to consideration of compliance costs in policy development:* The development of the Privacy Act gave explicit consideration to compliance costs and chose the model with the least costs. This model compares favourably with overseas privacy laws and meets current international privacy expectations.
- *Excessive complexity of regulations, processes and forms:* The Privacy Act gives maximum choice for agency compliance with it. There are no prescribed forms, registration, licensing or similar.
- *Failure to tailor compliance requirements to different types of business:* The mechanism of codes of practice was specifically introduced to cater to the needs of different types of business, as well as changing practices, technical developments and so on. The principles, along with their exceptions, take into consideration the different needs and circumstances of agencies. One-off exemptions can also be obtained. The Commissioner's education workshops and other initiatives tailor advice and information to specific sectors (such as health, education, employment and lawyers).
- *Lack of regular monitoring and review on the continuing need by government organisations for specific information requirements obtained by the private sector:* The Act does not require any information by government, unlike Australia where returns have to be filed and the UK which has a registration requirement. Principles 1 and 3 help to ensure that government agencies only ask for what is relevant and necessary (and are therefore a review mechanism imposed on government).¹⁹ In a broader sense, this Privacy Act review mechanism itself caters to this concern.
- *Insufficient explanation of the rationale for an obligation:* Principles 1 and 3 help in this regard by requiring government agencies to specify the purpose of collection of personal information.
- *Lack of information about what a measure means for individual companies:* As well as the Commissioner's enquiries and education work, codes of practice are tailored to industries and have been published with explanatory commentaries.
- *For individual businesses themselves, a lack of the management systems and skills necessary to comply:* While this is outside the direct control of the Act, it is able to be assisted by the education activities of the Privacy Commissioner.

The information privacy principles require agencies to question their practices and paperwork in relation to their use of personal information, eliminating unnecessary information and ensuring that the information used is sufficiently accurate for the purpose. All of these adjustments produce increased efficiency in the agencies' operations and tend to reduce costs (both internally and costs imposed on agencies through excessive or poorly designed information collection).

¹⁹ This point is further developed in a submission by the Privacy Commissioner to the Ministry of Commerce in relation to a Policy and Discussion Paper on Business Compliance Cost Reduction, 23 February 1995, reprinted in *Privacy: New Zealand*, Volume 3, p53.

SPECIFIC ISSUES

This paper has looked at the design of the Act, what it covers, particular compliance and administration costs features, and what the Privacy Commissioner does. The paper now turns to the particular sources of possible compliance costs and any issues arising from these. Few serious problems with the operation of the Privacy Act have been substantiated in either the public or private sectors.

In preliminary feedback elicited for this review there were few comments specifically related to compliance costs. Typical comments received include: "We are broadly satisfied with the way the Act has been working" and "Generally the Privacy Act has not been a burden". One submission explicitly pointed to compliance costs by way of specialist staff, extra training, additional forms and complaint handling procedures which affected its business, while at the same time recognising the value of the resultant enhanced rights for individuals. A few others regarded compliance with the principles as "unnecessarily complicated and problematic" and particularly commented about ignorance, a lack of commonsense, or overly strict, application of the Act. Deliberate misuse of the Act was also raised as a problem by several respondents.

A particular problem which has obscured other aspects of smooth implementation of the Act has been attributions that the Privacy Act sometimes prevents desirable disclosures of personal information. For example, it was claimed by some airlines that the Privacy Act prevented disclosure about details on passenger lists. Although restricting release was consistent with the Privacy Act, it would equally have been possible within the flexibilities provided by the Act for airlines to devise, publicise and implement a policy of release of details in particular circumstances. In fact airlines maintained a policy on non-disclosure before the Act and take the same approach in every country.

Another misunderstanding relates to the failure to realise that it is the Official Information Act, and its criteria, which apply to third party requests for information from a government agency.

Some misconceptions therefore prevail about the Act's true application (often compounded by continued inaccurate reporting) which has impeded the understanding of the Act in some agencies and by the public. Other agencies may actually be using the Act as an excuse for properly refusing to disclose information rather than taking responsibility for their information practices or to explain their reasons.

Another perceived problem has been "over compliance" or unduly cautious interpretations of the Act. For example, some agencies have been advised to seek clients' written authorisations when other acceptable, and less costly, options have been available.

The review of the Act provides an opportunity to explore options for solving problems of confusion or 'over compliance'. Solutions could include redrafting some provisions to make them easier to understand.

Layout and wording of Act

It is desirable that the Act, and the obligations which it imposes, are easily understood and interpreted consistently. The ease of interpretation and application of the Act can have a bearing on compliance costs. The complexity and presentation of legislation are key to this. The Law Commission's 1993 report *The Format of Legislation* recommended more modern statutory layout and plain English drafting.

It has been noted in some of the other discussion papers, for instance, that the marginal notes (headings) to principle 9 and section 27 are either unhelpful or misleading.

On the other hand, codes of practice issued under the Act use a relatively modern format and supply a commentary for guidance.

Suggestions are welcomed about specific areas or sections of the Act where improvements could be made. These matters are also addressed in other discussion papers (for example, in Discussion Paper No 1 Structure and Scope regarding definitions and layout).

Q5. Could the layout or wording of the Privacy Act be improved to make it easier to use?

Access requests

Individuals have rights to seek access to and correction of their personal information under principles 6 and 7 and Part IV of the Act. This is an area of the Act which holds potential for cost.

The Bankers' Association considered that there are significant costs arising from the provision of personal information even when that information is relatively accessible. Although this is debatable it raises in part the issue of who should bear any such costs, as between agencies and individuals. It also raises the question of how agencies organise information to reduce both the costs of retrieval and to enhance individuals' rights of access.

Personal information is in fact a vital asset of agencies and many of the information privacy principles provide the basis for good information handling practices. In addition, costs of collecting and holding information will often be incorporated into fees or other charges paid by individual clients.

Access and correction rights, where utilised, can sometimes help business to avoid problems by helping to ensure information is accurate, up to date, relevant and so on (using "individuals as first auditors"). Of course, some businesses, no doubt mindful of the overall advantages, were already allowing customers or employees access to their files. This had been a statutory requirement in the public sector. Public sector agencies may not charge individuals for giving access to their personal information.²⁰

²⁰ There is provision for the Commissioner to authorise public sector agencies to charge in certain circumstances set out in section 36.

While the access regime was familiar to the public sector under the Official Information Act 1982, it was new for the private sector. The Act allowed the private sector to make a reasonable charge for the provision of personal information to the individual concerned. The intention of this ability to charge was to minimise the cost to private sector agencies of meeting such requests. Reasonable charges may be made by private sector agencies for:

- the making available of information (cost of labour and materials);
- the correction of any information, including the attachment of a statement of correction; and
- the provision of assistance to the requester.

Charges cannot cover the making of the request, transfers of requests to other agencies, or the processing of the request, including deciding whether or not the request is to be granted and, if so, in what manner.

This issue is dealt with further in Discussion Paper No 3 on access and correction.

Q6. Should more cost recovery for access and correction requests be allowed to reduce agencies' compliance costs?

Complaints

The Bankers' Association expressed concern that the time taken by the Privacy Commissioner to resolve complaints, which it considered currently to be excessive, contributed to higher compliance costs. At present non-urgent complaints at present wait up to eight months for an investigation to begin. This is an issue related to resources provided to the Commissioner's office which perhaps demonstrates the link between administration costs and the costs incurred by agencies. It may be appropriate to characterise public money spent on funding the complaints processes as bearing costs which would otherwise fall on individuals *and* agencies.

However, there is also a responsibility on agencies to deal with areas giving rise to complaints and to try to resolve them at an early stage. In fact some industries which centre on personal information have incurred compliance costs in voluntarily assuming at their own cost certain code and complaint mechanisms, such as the banking and insurance ombudsman schemes, for which the industries see an overall benefit.

Issues about complaints are raised in Discussion Paper No 6 on complaints and investigation.

Q7. How do any delays in dealing with complaints affect compliance costs? What measures could reduce the time for complaints investigation and resolution to reduce compliance costs?

Privacy officers

Each agency must have at least one privacy officer to encourage compliance with the privacy principles, to deal with requests for information and to work with the

Commissioner in relation to investigations of complaints (section 23). In many agencies this role will be combined with other information handling or compliance roles. This can have an advantage over having legal advisers involved.²¹

Q8. Can the privacy officer's role be enhanced in some way relevant to effective use of resources in regard to compliance?

Q9. What specific compliance costs incurred are of most concern? In what ways could these be reduced?

Q10. Overall, what do you think about the extent of compliance costs incurred by the Privacy Act? Are they excessive, just about right, or is the Act in fact helpful in reducing compliance or other costs?

Advance rulings

There have been calls at times for the Commissioner to be authorised to make advance rulings in relation to the privacy implications of new proposals or products.

There have also been some calls for more specific statutory provisions in the Act setting out what agencies may or may not do. However, the New Zealand approach has not been to provide tightly prescribed requirements but instead allow maximum choice in how to comply with the Act. Such "lighthanded" regulation allows business to make their own decisions; with this comes a certain amount of risk and uncertainty.

Other mechanisms which the Act provides, such as codes of practice and exemptions,²² may serve an equivalent role to advance rulings. The Australian Business Licences and Regulatory Reform report noted that businesses may be less likely to comply with a prescriptive approach than with a code of practice developed consultatively. It observed that such arrangements lack flexibility and may fail to keep pace with developments in information technology.

The Commissioner has taken the position that it is not desirable to make such advance rulings as it would interfere with his independent role in relation to complaints investigation should there later be a complaint. Any useful and dependable ruling would require that full information would have to be provided at the outset. It is most likely that rulings would be desired for products which are borderline or where a privacy-friendly or cautious approach is being disregarded for one which makes unexpected use of personal information. These are the very cases in which the Commissioner would be the least willing to give clearances. They are also the cases where the Commissioner may be most wary as to whether the explanations put before him about the proposal are complete or accurate.

²¹ A recent review of the Nova Scotia privacy legislation recommended that agencies such as schools and hospitals be urged to designate staff members to be administrators rather than directing access requests to legal advisers. See Nova Scotia Department of Justice, Advisory Committee Freedom of Information & Protection of Privacy Act Report, March 1996.

²² See sections 46 and 54 of the Act respectively.

Most businesses should be well capable of analysing most of the Privacy Act compliance issues relating to any proposed scheme and, if necessary, they can obtain expert advice. If the Privacy Commissioner were to become involved in giving advance rulings, and the Act gave them some recognition, it would be necessary to go thoroughly into a proposal and to have powers to find out the information needed and to obtain any necessary expert advice (such as on computer security safeguards on a product for which that feature was important). Since some proposals may be entirely novel, research might be necessary. This would be a more expensive proposition than people usually contemplate when talking of Commissioner "pre-approvals" or "rulings".

The approach of the Privacy Act has been for agencies to choose how to comply with it, rather than having to seek permission or be told what to do. The Act is concerned with outcomes rather than how they must be achieved.

Q11. Would advance rulings help reduce compliance costs? Can such rulings achieve the advantages expected of them? Are the disadvantages too severe to be worthwhile?

Specific exemptions

There may be scope to further develop flexible mechanisms tailored to the specific needs or circumstances of individual agencies or sectors. For example, the Privacy Commissioner's power to grant exemptions under section 54 could be extended beyond actions which would otherwise breach principles 2, 10 or 11 to include principles 9 and 12. This issue and others are discussed in Discussion Paper No 4 codes of practice and exemptions.

Q12. Are there other mechanisms which could usefully cater for the specific needs and practices of agencies or sectors to reduce compliance costs?

Any other suggestions to further reduce compliance costs are welcomed.

The Privacy Commissioner may include in his final report a list of submissions received. He may also refer to submissions in the text of his report. If you want your submission or any part of it treated confidentially, or do not want it used in this way, please indicate this clearly. The Commissioner is subject to the Official Information Act. Copies of submissions may therefore be released on request. Any request for the withholding of information on the grounds of confidentiality or for any other reason will be determined in accordance with that Act and section 116 of the Privacy Act.

act-revi/disc/discppr9