

COMPLIANCE COSTS AND THE PRIVACY ACT 1993: PERCEPTION OR REALITY FOR ORGANISATIONS IN NEW ZEALAND?

*Emma Harding**

This article looks at compliance costs under the Privacy Act 1993. It draws on the findings of previous "general" compliance cost surveys as a basis for analysis of the author's own recent survey entitled "Compliance Costs and the Privacy Act 1993". There is a widespread perception amongst the business community that compliance costs under the Privacy Act are "excessive". However, the findings of the author's survey show that this is not the reality in New Zealand. The article highlights some of the key concerns businesses have relating to compliance costs under the Privacy Act and suggests ways in which these could be minimised. Specifically, the article recommends that the current charging regime under section 35 should be removed from the Act thereby prohibiting all agencies from charging for costs incurred in relation to information privacy requests. Additionally, the article advocates continuing education to displace some commonly held misconceptions about the Act. There should be a focus on encouraging compliance with section 23 of the Act (which requires agencies to have at least one privacy officer). This discussion is located within the context of a broad definition of compliance costs, including direct business costs as well as intangible and non-quantifiable costs imposed on an organisation by legislation.

I INTRODUCTION

Compliance costs arising from legislative enactments have been an issue for governments around the world for many years. Economists argue that governments should minimise compliance costs imposed by legislation as much as possible because there is a negative impact on society and the economy where these costs are excessive. For instance,

* Submitted as part of the LLB(Hons) programme at Victoria University of Wellington. The author now works as a solicitor at Chapman Tripp in Wellington and can be contacted at emma.harding@chapmantripp.com.

excessive compliance costs can discourage growth and employment,¹ and they may discourage organisations from complying with legislation.²

Perceptions of compliance costs as well as the actual impact of these costs on business can influence an organisation's decision to expand operations and also its choice to comply with legislation. In fact, perception can be as important as reality.

There is a widespread opinion amongst the business community that compliance costs are too high. This seems to be particularly prevalent among small to medium sized businesses (businesses having fewer than 19 employees),³ which make up 95 per cent of the total number of businesses in New Zealand.⁴ Recent research has confirmed that, in general, this perception mirrors reality. These studies have shown that the compliance burden is much higher for small rather than large businesses because they are less able to absorb such expenses.⁵ In particular, taxation, health and safety, and employment legislation are commonly cited as the types of enactments imposing the greatest compliance costs on business.⁶ This may be due to the complexity of these pieces of legislation. The more complex legislation is, the greater the direct costs for organisations to interpret its provisions and ensure their practices comply with the requirements of the legislation. Also, the payout of the legislation may make it hard for lay people to follow.⁷ Additionally, the

-
- 1 Office of the Privacy Commissioner *Review of the Privacy Act 1993: Discussion Paper 9 (Compliance and Administrative Costs)* (Wellington, 1997) 6 [*Discussion Paper 9*].
 - 2 Rt Hon Bill Birch MP, Minister of Finance *Business Compliance Cost Reduction: A Government Policy and Discussion Paper* (Wellington, 1994) 6.
 - 3 Ceri Jones, Firm Capability Team, Ministry of Commerce *SMEs in New Zealand: Structure and Dynamics* (Ministry of Commerce Report, Wellington, 1999) 4, although this report acknowledges the difficulty in finding a globally recognised definition of a small to medium sized enterprise (SME).
 - 4 Ministry of Economic Development *Business Compliance Cost Statements: Guidelines for Departments* (Wellington, 2001) 4 [*Business Compliance Cost Statements*].
 - 5 See for example, Auckland, Wellington, and Otago Chambers of Commerce *Red Tape Survey* (Auckland, 2004) [*Red Tape Survey*]; W R J Alexander, John D Bell and Stephen Knowles *Quantifying Compliance Costs of Small Businesses in New Zealand* (School of Business, University of Otago, Dunedin, 2004); Business NZ-KPMG *Business New Zealand-KPMG Compliance Cost Survey* (Wellington, 2004) [*Business New Zealand-KPMG Compliance Cost Survey*].
 - 6 *Red Tape Survey*, above n 5; *Business New Zealand-KPMG Compliance Cost Survey*, above n 5; Alexander, Bell and Knowles, above n 5.
 - 7 Office of the Privacy Commissioner *Necessary and Desirable: Privacy Act 1993 Review (Report of the Privacy Commissioner on the First Periodic Review of the Operation of the Privacy Act)* (Auckland, 1998) [*Necessary and Desirable*] para 1.2.5 specifically considered ways in which the layout of the Act could be made more "user friendly" to ordinary people."

substance of the legislation (for example, language used) may be complex, overly technical or unnecessarily vague so that organisations have to seek costly legal advice to determine their obligations under the legislation.⁸

With the notable exception of one survey,⁹ these general studies on compliance costs in New Zealand do not expressly refer to the Privacy Act 1993 (the Act). The survey questions do not refer to the Act and the responses do not comment on compliance costs imposed by the Act. Yet, anecdotally, there are assertions of burdensome compliance costs under the Act.

The difference between these assertions and the omission to mention the Act in these studies could be accounted for by the fact that they had a general focus. Results from a general survey will focus on the compliance costs arising with regard to those enactments that traditionally impose the greatest burden on businesses. Legislation such as the Privacy Act may in fact impose excessive compliance costs but since these costs are not as high (in nominal terms) as those imposed by taxation legislation, for example, these concerns may not feature in respondents' answers, even though they may still be an issue. Therefore, it is unclear how reliable the results of these general surveys are with regard to pieces of legislation, such as the Privacy Act, that are not as prominently associated with compliance costs as taxation legislation is. Further research is needed to determine whether the omission to mention the Act means that businesses have no concerns with this legislation or whether they have concerns but these issues are more minor than those associated with other enactments.

Hence, there is a need for "specific" surveys focusing on particular enactments such as the Privacy Act. Respondents to surveys that are targeted to specific pieces of legislation will have the target enactment at the forefront of their minds rather than issues associated with the traditional "problematic" pieces of legislation. In relation to the Act, only one such study has previously been conducted in New Zealand. In 1997 the then Privacy Commissioner (the Commissioner), Bruce Slane, released 12 discussion papers pursuant to the requirement that the Act's operation be reviewed at certain intervals.¹⁰ One of these discussion papers focussed solely on compliance and administration costs.¹¹ The findings to

8 Many small to medium sized enterprises prefer to rely on guidelines and other material printed by the Office of the Privacy Commissioner rather than attempt to interpret the Act's provisions on their own: Author's "Privacy Act 1993 Compliance Costs Survey" Business Professional Services Limited response (14 July 2004).

9 Ministerial Panel on Business Compliance Costs *Finding the Balance: Maximising Compliance at Minimum Cost* (Ministry of Economic Development, Wellington, 2001) [*Finding the Balance*].

10 Privacy Act 1993, s 26.

11 *Discussion Paper 9*, above n 1.

come out of this study are summed up in the following submissions received in response to these discussion papers:

... [O]ur members do not report any major difficulties and have found that compliance is largely a matter of good business practice;¹²

Compliance costs seem to be reasonably efficient and minimal and the Act quite flexible in this respect;¹³

... [W]hile at an anecdotal level there are assertions of burdensome compliance costs, few organisations are able to substantiate these claims with concrete evidence that the Privacy Act imposes long-term compliance costs, beyond that expected from appropriately targeted regulation.¹⁴

The Commissioner's study and subsequent report provided the impetus for my survey. I wanted to assess whether the regulatory burden faced by businesses complying with the Act was still minor in 2004. My survey differed from previous research in that it was specifically focussed on the Privacy Act rather than all legislation in general. Additionally, it differed from the Commissioner's discussion paper released in 1997 in that it was sent to targeted organisations rather than inviting submissions from the public. Furthermore, it was a completely independent study not conducted by a business interest group, that may have a vested interest in the outcome.

I conducted my survey by sending out a questionnaire entitled "Privacy Act 1993 Compliance Costs Survey"¹⁵ to 50 New Zealand organisations. This questionnaire consisted of 12 open-ended, general questions. This survey group included both large and small enterprises.¹⁶ The organisations selected were those who made submissions on the Commissioner's discussion paper in 1997 as well as other similar organisations chosen at my discretion. From the questionnaires sent, there was a 20 per cent return rate.¹⁷ Although the

12 Office of the Privacy Commissioner *Review of the Privacy Act 1993: Compliance Cost Submissions* (Auckland, 1998) [*Compliance Cost Submissions*] Insurance Council of New Zealand submission L9 (date not cited).

13 *Compliance Cost Submissions*, above n 12, New Zealand Association of Social Workers Aotearoa WX 4 (23 October 1997).

14 *Compliance Cost Submissions*, above n 12, Ministry of Justice WX 11 (December 1997).

15 A copy of the questionnaire questions is included in Part VII Appendix One.

16 A copy of the list of organisations that responded to the questionnaire is listed in Part VIII Appendix Two.

17 This equated with 10 surveys returned out of 50 mailed.

relatively low response rate limits the general applicability of my findings,¹⁸ the responses received allow some measure of analysis.¹⁹

Despite the anecdotal evidence of compliance costs under the Act, the results of my survey confirm the Commissioner's earlier findings that the Act does not impose major compliance costs on organisations in New Zealand.

This article begins its analysis of the findings of my research with a general discussion about the interest in compliance costs: why are they such a concern and how much of a current issue are they? Unfortunately there is little general academic discussion on compliance costs. Most textbooks tend to specifically focus on tax compliance costs, which is a discrete subject. However, this article will draw on discussion and analysis from reports and surveys about compliance costs to highlight the reasons why they are an important area requiring research and debate.

In order to assess compliance costs under the Act, it is first necessary to consider the different types of compliance costs. This is no easy task but is broadly developed in Part III and provides a foundation for the later analysis. After discussing the relevant background to the Act, the article highlights specific examples of compliance costs under the Act as raised by respondents to the questionnaire. These examples are section 35 (the charging regime) and section 23 (the privacy officer requirement). This discussion assumes that the Act has certain benefits and instead focuses on the impact of the costs it imposes. The article considers ways in which the Act could be amended or how practices under the Act could be changed to minimise the compliance costs identified. Specifically, the article will argue that education is the key to reducing compliance costs under the Act.

II INTEREST IN COMPLIANCE COSTS

A Economists and Governments

Legislation is an essential factor in helping government achieve its economic, social and environmental goals.²⁰ It is acknowledged by businesses that some degree of regulation is

18 As these survey findings were not being used for statistical purposes, no tests for response bias were conducted. One would expect that a survey of this nature would be biased towards results showing large compliance costs. The reason for this is that people who are concerned about compliance costs under the Act are more likely to respond to a questionnaire of this sort. However, my survey findings were interesting in this regard in that they were biased in the other direction: that is, those responding generally had very little issues with compliance costs.

19 A less than 30 per cent response rate on a mail out survey is not ideal but a response rate greater than 15 per cent is useable both statistically and qualitatively: W Lawrence Neuman *Social Research Methods: Qualitative and Quantitative Approaches* (Allyn and Bacon, Needham Heights (Mass), 1991) 192-193.

20 *Business Compliance Cost Statements*, above n 4, 3.

necessary and the costs of complying with legislation are concomitant to doing business in New Zealand.²¹ Compliance with legislation is "an integral part of being a responsible employer and of being a good member of the community".²² Most government interventions in the economy impose certain inevitable costs of compliance on organisations. These are commonly known as "compliance costs".²³ Sometimes such costs are entirely justifiable as being necessary to achieve the aims of the legislation. However, it is when costs are "excessive" that economists become concerned.

Costs can be seen as "excessive" where it "would be practicable to achieve the essential objectives of ... legislation without all or part of the costs actually encountered".²⁴ In other words, in economic jargon, excessive costs arise where the legislation is "inefficient". In economics, something is "inefficient" where one person can be made better off without making any other person worse off.²⁵

However, the New Zealand Business Roundtable argues that this definition of "excessive" is too narrow.²⁶ This interest group, and other economists, emphasise the need to consider both the costs and benefits of proposed legislation.²⁷ In other words, the principles of the Act should not be taken as given, but rather should be subject to a cost-benefit analysis.²⁸ Where the costs to business of complying with the regulation are

21 *Finding the Balance*, above n 9, para 1.4.

22 *Finding the Balance*, above n 9, para 1.4.

23 See Part III Different Types of Compliance Costs for a discussion about the different aspects to the term "compliance costs".

24 *Discussion Paper 9*, above n 1, 5.

25 In economic jargon, this is known as Pareto efficiency or allocative efficiency and is one of several economic definitions of efficiency: see, for example, Robert Cooter and Thomas Ulen *Law and Economics* (4 ed, Pearson Addison Wesley, Boston, 2004) 16.

26 *Compliance Cost Submissions*, above n 12, New Zealand Business Roundtable S50 (10 November 1997) 130.

27 *Compliance Cost Submissions*, above n 12, New Zealand Business Roundtable S50 (10 November 1997) 130; Alexander, Bell and Knowles, above n 5, 5. See also Senate Legal and Constitutional Committee *Privacy in the Private Sector: Inquiry into Privacy Issues, Including the Privacy Amendment Bill 1998* (Canberra, 1999) para 8.24, which recommends that any proposal for new legislation be subject to a cost-benefit analysis "to ensure that costs are not unreasonable in the context of the social objective of the legislation".

28 *Compliance Cost Submissions*, above n 12, New Zealand Business Roundtable S50 (10 November 1997) 130; supported by section 14(a) of the Privacy Act 1993 which requires the Privacy Commissioner to "have due regard for the protection of human rights and social interests that compete with privacy, including the general desirability of a free flow of information and the recognition of the right of government and business to achieve their objectives in an efficient way".

disproportionately high compared to the benefits of the legislation to both society and businesses, then compliance costs are said to be "excessive".²⁹

Whilst it used to be common for new legislation to be subject to a cost-benefit analysis before being introduced to the House, it has only recently been mandatory to expressly consider compliance cost implications. Since 1 April 2001 all policy proposals submitted to Cabinet that have compliance cost implications for business must include a Business Compliance Costs Statement (BCCS).³⁰ The aim of the BCCS is to help ensure that compliance costs are fully considered and "kept as low as possible".³¹

Despite government aspirations to minimise compliance costs, this is not always achieved, with potentially detrimental effects on the economy. Specifically, excessive compliance costs divert resources away from the core interests the business is engaged in.³² This leaves less money for expansion and investment in research and development, for example.

Furthermore, over-burdensome compliance costs can discourage businesses from complying with the underlying legislative enactment.³³ Where this is coupled with negligible penalties for non-compliance, businesses that do comply are comparatively competitively disadvantaged. If costs result in widespread non-compliance with the underlying legislative enactment, the purpose of the legislation is undermined. This is discussed further in the context of section 23, which requires each agency to appoint a privacy officer.³⁴

Economists argue that not only is it important to reduce compliance costs in order to prevent their potential detrimental effect on the economy but it is also important to address the disproportionately heavy burden that they place on small to medium sized enterprises.³⁵ The amount of resources needed to comply with legislation may bear little relation to the

See also discussion in *Necessary and Desirable*, above n 7, para 3.4.3 where it is emphasised that privacy must be balanced against competing interests.

29 *Compliance Cost Submissions*, above n 12, New Zealand Business Roundtable S50 (10 November 1997) 130.

30 *Business Compliance Cost Statements*, above n 4.

31 *Business Compliance Cost Statements*, above n 4, 3.

32 *Finding the Balance*, above n 9, 31.

33 *Finding the Balance*, above n 9, 31.

34 See Part IV C Privacy Officer Requirement.

35 *Business Compliance Cost Statements*, above n 4, 4.

size of the organisation.³⁶ For example, the requirement under section 23 of the Act for each agency to have a privacy officer places a much higher cost on a small to medium sized enterprise than it does on a large business. Additionally, small to medium sized enterprises are less able to employ specialist staff to advise on their obligations under the Act, which can affect their ability to comply with the Act because the owner may not be aware that there is a breach of the Act's provisions.

Failure to acknowledge the different impact of costs on small to medium sized enterprises compared to large ones is one of the ways in which legislation can cause excessive compliance costs.³⁷ Other causes of excessive compliance costs cited by the Ministry of Economic Development and relevant to the discussion in this paper are:³⁸

- overly complex regulations, processes and forms;
- lack of regular monitoring of legislation;
- not enough explanation of the rationale or justification behind a particular obligation; and
- inappropriate, insufficient, or inaccessible information about the key features of obligations and what they mean for individual organisations.

B Compliance Costs Surveys

To assess whether legislation minimises compliance costs effectively, empirical research is necessary. In contrast to the relative lack of theoretical and academic discussion about compliance costs in general, in recent years there seems to have been a proliferation of surveys in New Zealand that assess the practical reality of the regulatory burden. Commonly, compliance costs surveys are of a general nature, seeking to assess the compliance burden on businesses from all legislation.

The Auckland, Wellington and Otago Chambers of Commerce published a general compliance cost survey in August 2004.³⁹ The narrow focus of this survey meant that respondents were not asked to consider the impact of compliance costs under the Act; nor were they given an opportunity to highlight additional costs that were not the subject of

³⁶ *Business Compliance Cost Statements*, above n 4, 4; Cedric Sandford and John Hasseldine *The Compliance Costs of Business Taxes in New Zealand* (Institute of Policy Studies, Wellington, 1992) 12.

³⁷ *Business Compliance Cost Statements*, above n 4, 5.

³⁸ *Business Compliance Cost Statements*, above n 4, 5.

³⁹ *Red Tape Survey*, above n 5.

specific questions in the survey.⁴⁰ Therefore, it was not surprising that the Act did not receive a mention in the published report.

Also in August 2004, Business NZ and KPMG jointly published a general New Zealand compliance cost survey. This was the second annual survey on business compliance costs conducted by these organisations. Nearly all the firms they surveyed perceived their compliance problem to have either worsened or stayed the same.⁴¹ Even though privacy legislation is cited as raising significant costs, as demonstrated in Australia,⁴² compliance costs associated with the Privacy Act do not receive a mention in this survey. Compliance costs associated with taxation, employment and environmental legislation overshadow any issues organisations have with compliance costs and the Act. Even in the section asking for "other compliance costs" faced by organisations, the Privacy Act was not mentioned by even one respondent.

Furthermore, previous research studies such as the University of Otago's School of Business *Quantifying Compliance Costs of Small Businesses in New Zealand* in June 2004,⁴³ and the New Zealand Centre for Small and Medium Enterprise Research's report prepared for the Ministry of Economic Development in May 2003,⁴⁴ also do not mention the Privacy Act in their findings. This does not necessarily mean that the Act does not impose significant costs on businesses. Their scope is limited and the methodology employed by the researchers may not invite responses about the Act. In the case of the University of Otago survey, the study sample was limited to businesses operating as cafes, engineering firms, garages, hairdressers and motels.⁴⁵ With the possible exception of the last two types of businesses, these industries are not renowned for collecting large quantities of personal information. Hence, compliance with the Privacy Act would not be a priority for them. Similarly, the New Zealand Centre for Small and Medium Enterprise Research's report recognises its limitation in not covering all areas of regulation.⁴⁶

40 Auckland Chamber of Commerce "Red Tape and Compliance Costs Clearly Stifle Business Growth" (9 September 2004) Press Release; Auckland Chamber of Commerce "New Zealand's Small Business Sector Crushed by the Cost of Compliance" (9 September 2004) Press Release.

41 Business New Zealand-KPMG "Small Firms Still Worst Hit by Compliance Costs" (26 August 2004) Press Release.

42 This is discussed in the next section, Part II C Australia.

43 Alexander, Bell and Knowles, above n 5.

44 Clare Massey, New Zealand Centre for Small and Medium Enterprise Research, Massey University *The Impact of Business Compliance: Perceptions of New Zealand Firms* (Prepared for the Ministry of Economic Development, Wellington, 2003) 1.

45 Alexander, Bell and Knowles, above n 5, 9.

46 Massey, above n 44, 1 footnote 2.

In contrast to that research, one study undertaken in 2001 indicates that the Privacy Act *does* in fact impose compliance costs on organisations, even if these are negligible in most circumstances.⁴⁷ Even though this was a general study, given its comprehensive nature and the fact that it assessed the majority of legislation then in force for compliance cost implications, it is not surprising that the Act was mentioned. A Ministerial Panel on Business Compliance Costs (the Panel) set up in December 2000 by the Minister of Commerce and the Minister of Finance conducted this research. The Panel were required to "identify the key areas where unnecessary and excessive compliance costs occurred, prioritise the areas for action and provide workable and practical solutions".⁴⁸

The findings of the Panel's research showed that the Act raised *some* issues for businesses, even though these were not a key concern. In particular, while businesses thought that the principles of the Act were "commendable", they found that the Act did not assist them in applying the principles in everyday work practice.⁴⁹ Three main concerns in relation to the Act came out of the research:⁵⁰

- uncertainty about the requirements of the Act;
- lack of clear guidelines about the duties of privacy officers; and
- conflict between the Act and other legislation.

In particular, businesses were concerned about the amount of time they had to spend trying to determine correct approaches or having to seek costly legal advice due to uncertainty about the Act's requirements.⁵¹ For instance, employers were uncertain about what questions they were allowed to ask prospective employees and were unclear about whether the Act imposed restrictions on their ability to disclose information about employees during due diligence.⁵²

⁴⁷ *Finding the Balance*, above n 9.

⁴⁸ *Finding the Balance*, above n 9, para 1.2 (emphasis omitted).

⁴⁹ *Finding the Balance*, above n 9, para 6.8.2.

⁵⁰ *Finding the Balance*, above n 9, para 6.8.3.

⁵¹ *Finding the Balance*, above n 9, para 6.8.3.

⁵² The Privacy Act 1993 is not the only statute placing restrictions on what questions employers ask and what information they are allowed to collect about employees. Employers also have to take care to ensure they comply with the Human Rights Act 1993. In particular section 23 of the Human Rights Act 1993 provides that it is unlawful for "any person to use or circulate any form of application for employment or to make any inquiry of or about any applicant for employment which indicates, or could reasonably be understood as indicating, an intention to commit a breach of section 22 of this Act." Section 22 makes it unlawful for an employer to discriminate against an employee on one of the prohibited grounds of discrimination contained in section 21, which

Additionally, this study found that there appeared to be a general lack of knowledge, particularly among small and medium enterprises, about the requirement for businesses to have a privacy officer.⁵³ Where businesses were aware of this requirement many were uncertain about the duties of privacy officers.⁵⁴

The final finding of the Panel's study in relation to the Act was that there was confusion among businesses about which legislation prevailed where the Act conflicted with another enactment.⁵⁵ This confusion commonly occurred where there was a conflict between the Official Information Act 1982 (the OIA) and the Privacy Act, or where the Privacy Act limited disclosure of information that was legally sought by government agencies such as the Accident Compensation Corporation and the Inland Revenue Department.⁵⁶

The Panel recommended the following practical amendments to reduce compliance costs under the Act:⁵⁷

- prepare step-by-step guidelines and make them available on the Privacy Commissioner's website and to industry associations;
- fully staff the Privacy Commissioner's 0800 helpdesk during normal work hours; and
- provide constructive advice to business on how to comply in practice.

The Ministry of Economic Development (MED) made these recommendations in their report written in December 2001.⁵⁸ However, they noted that the Commissioner had already implemented the last two of these recommendations.⁵⁹

include: sex or sexual orientation, marital status, religious or ethical belief, colour, race, ethnic or national origins, disability, age, political opinion, employment or family status. In this way the Privacy Act 1993 interacts with the Human Rights Act in the area of restricting collection of personal information.

53 *Finding the Balance*, above n 9, para 6.8.3.

54 *Finding the Balance*, above n 9, para 6.8.3. My survey found that this still represented the reality for a majority of organisations in 2004. This is discussed in greater detail below at Part IV C Privacy Officer Requirement.

55 *Finding the Balance*, above n 9, para 6.8.3.

56 *Finding the Balance*, above n 9, para 6.8.3.

57 *Finding the Balance*, above n 9, para 6.8.3.

58 Ministry of Economic Development *Striking the Balance: Government Response to the Ministerial Panel on Business Compliance Costs* (Wellington, 2001) [*Striking the Balance*].

59 In June 2003, MED reported that subsequent to December 2001 the Commissioner had made step-by-step guidelines available on the Office of the Privacy Commissioner's website, as well as

Despite the findings in these surveys, there is still a perception amongst the business community in New Zealand that compliance costs under the Privacy Act are unreasonably high. This is similar to the position in Australia where perception and actual incidence of these costs appear to be different.

C Australia

Compliance costs and privacy legislation are currently in the spotlight in Australia. From 1990, the Privacy Act 1988 (Cth) (the Australian Act) regulated the Commonwealth and ACT public sectors but it only covered private sector credit providers and credit reporters.⁶⁰ Following international pressure, mainly from the European Union, the Commonwealth Government released a Discussion Paper entitled *Privacy Protection in the Private Sector* in September 1996.⁶¹ However, in March 1997, Prime Minister John Howard announced that the Government had decided against extending the Australian Act to cover private sector organisations.⁶² The only reason cited for this decision was that such a move would "further increase compliance costs for all Australian business, large and small".⁶³

This decision was made by the Australian Prime Minister notwithstanding research showing the contrary to be the reality in Australia. Price Waterhouse's 1997 "Privacy Survey" showed that contrary to politicians' and some vocal organisations' assertions, the reality for major Australian businesses, like their New Zealand counterparts, is that privacy legislation does not impose significant compliance costs.⁶⁴

producing a publication in both electronic and hard copy formats entitled "Privacy Impact Assessment Handbook": Ministry of Economic Development *Business Compliance Costs Perception Survey* (Wellington, 2003) [*Business Compliance Cost Reduction Report-Back*].

- 60 When it was enacted, the Australian Act only regulated public sector agencies: Privacy Act 1988 (Cth), s 6 definition of "agency". However, the Privacy Amendment Act 1990 extended coverage of the Australian Act to credit providers and credit reporters by amending section 7 of the Australian Act, which (after amendment) additionally provided that the Act covered acts done or practices engaged in by credit providers or credit reporters.
- 61 Commonwealth Government of Australia *Privacy Protection in the Private Sector* (Canberra, 1996). Also discussed in Daryl Williams, Commonwealth Attorney-General "Privacy and the Private Sector" (1996) 3 PLPR 81.
- 62 Graham Greenleaf "Commonwealth Abandons Privacy – for Now" (1997) 4 PLPR 1.
- 63 John Howard, Australian Prime Minister "Privacy Legislation" (21 March 1997) Press Release, as cited in Graham Greenleaf "Commonwealth Abandons Privacy – for Now" (1997) 4 PLPR 1, 1.
- 64 Graham Greenleaf "70 per cent of Companies Support Privacy Laws – Price Waterhouse Survey" (1997) 4 PLPR 21; for full survey see "Price Waterhouse Privacy Survey 1997" (1997) 4 PLPR 22, 27. Seventy five per cent of respondents stated that their organisation would only require minor process re-engineering, if change was required at all, to comply with privacy legislation in the

Compliance costs and privacy legislation were again thrust into the spotlight in September 1999 when the Commonwealth Attorney-General's Department issued a consultation paper entitled *The Government's Proposed Legislation for the Protection of Privacy in the Private Sector*.⁶⁵ The Privacy Amendment (Private Sector) Act 2000 (Cth) (the amending Act) resulted from this discussion paper, and came into force on 21 December 2001. It extended the coverage of the Australian Act to all businesses with an annual turnover of at least AUD\$3 million.⁶⁶ However, it provided exemptions for employee records,⁶⁷ political parties when engaged in political activities,⁶⁸ and the media.⁶⁹ The large number of exemptions indicates the government's key concern to minimise compliance costs as much as possible. The Australian Federal Government's own figures show that the extent of the exemptions mean that 94 per cent of all Australian businesses are not regulated by the Act.⁷⁰ Arguably, therefore Australia's efforts to minimise compliance costs came at the expense of privacy protection.

This has been confirmed in a recent report entitled *Getting in on the Act: the Review of the Private Sector Provisions of the Privacy Act 1988* written by the Australian Government's Office of the Privacy Commissioner, which showed that "the failure of the private sector provisions to meet their objective of national consistency in privacy regulation

private sector. The survey authors conclude that this illustrates that many organisations believe that their current business practices are sufficient to comply with any form of privacy legislation.

- 65 An edited version of this paper appears in "Commonwealth Proposals for Private Sector Privacy" (1999) 6 PLPR 2; further discussion about this consultation paper as well as the submissions made in response to it can be found at "Privacy in the Private Sector: History of the Privacy Amendment (Private Sector) Act 2000" <<http://www.ag.gov.au/agd>> (last accessed 10 October 2005).
- 66 Privacy Act 1988 (Cth), s 6D defines a "small business" as a business having an annual turnover of \$3,000,000 or less for the previous financial year and a "small business operator" as a body corporate, trust or individual carrying on one or more small businesses. Section 16 of the Australian Privacy Act 1988 (Cth) provides that agencies are to comply with the privacy principles and "agency" is defined in section 6 as including an "organisation", which is defined in section 6C(1) as excluding small business operators. Therefore, small businesses do not need to comply with the national privacy principles and, therefore, the Australian Act.
- 67 Privacy Act 1988 (Cth), s 7B(3).
- 68 Privacy Act 1988 (Cth), s 7C.
- 69 Privacy Act 1988 (Cth), s 7B(4).
- 70 House of Representatives Standing Committee on Legal and Constitutional Affairs *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (Canberra, 2000) para 2.20 as cited in Patrick Gunning "Central Features of Australia's Private Sector Privacy Laws" [2001] Cyber L Res 2. Note, however, the government believes that the remaining six per cent of Australian businesses are responsible for approximately 70 per cent of total sales made in Australia.

has had consequences for business efficiency".⁷¹ This lack of consistency "has posed some impediments in the way of individuals seeking to have their privacy rights respected".⁷² The Report recommends modifying the small business exemption to simplify its application⁷³ and suggests that some sectors with high privacy risks should be covered by the private sector provisions.⁷⁴

Overall, though, the Report concluded that there is no fundamental flaw with the private sector provisions in the Australian Act⁷⁵ nor with costs associated with complying with the Australian Act. One submitter reported "significant disruption and cost with the original implementation" of the Act but this organisation found that ongoing compliance costs were relatively small.⁷⁶ Similarly, another submitter stated that the Australian Act "sets out little more than reasonably sensible data management practice".⁷⁷

III DIFFERENT TYPES OF COMPLIANCE COSTS

Defining "compliance" costs is not as straightforward as one might think. There is no statutory definition of the term. Business New Zealand defines⁷⁸ it as "the administrative and paperwork costs businesses incur when meeting a regulatory obligation".⁷⁹ While this definition is a good starting point for considering compliance costs, it does not fully capture the true extent of such costs.

71 Office of the Privacy Commissioner *Getting in on the Act: the Review of the Private Sector Provisions of the Privacy Act 1988* (Canberra, 2005) 4 [*The Review of the Private Sector Provisions of the Privacy Act 1988*]

72 *The Review of the Private Sector Provisions of the Privacy Act 1988*, above n 71, 4.

73 The Report recommends expressing the definition of "small business" in terms of number of employees (20 employees or fewer) rather than annual turnover: *The Review of the Private Sector Provisions of the Privacy Act 1988*, above n 71, 15.

74 *The Review of the Private Sector Provisions of the Privacy Act 1988*, above n 71, 7. Sectors with high privacy risks cited by the Report include tenancy databases and telecommunications sectors.

75 *The Review of the Private Sector Provisions of the Privacy Act 1988*, above n 71, 2-3.

76 *The Review of the Private Sector Provisions of the Privacy Act 1988*, above n 71, 172: Investment and Financial Services Association Limited.

77 *The Review of the Private Sector Provisions of the Privacy Act 1988*, above n 71, 172: Australian Consumers' Association.

78 Business New Zealand is the policy and advocacy wing of various regional employers' business associations.

79 Author's "Privacy Act 1993 Compliance Costs Survey" Business New Zealand response (1 July 2004).

Commonly it is thought that compliance costs are limited to those monetary costs arising directly from an agency's compliance with an enactment or regulation. It is clear, however, that direct costs incurred by an organisation in complying with legislation are not the only costs included in the scope of the concept. The need to comply with the requirements of legislation can also have non-quantifiable and intangible effects.

A Direct Business Costs

"Direct business costs" can be broken into two types: establishment costs and ongoing costs of complying with legislation. Generally there is a trade-off between establishment and ongoing costs. For instance, a new enactment may impose high "one-off" establishment costs such as setting up a computerised programme to file documents in the correct format with a government agency. However, the ongoing costs to comply with this legislation will be reduced as forms do not need to be filled out manually and a report in the correct format can be completed "with the click of a button". When looking at compliance costs it is important to consider the total impact of both types of business costs.

It is acknowledged that for credit reporting agencies, such as Baycorp, whose business it is to sell personal information, any regulation of the handling of personal information will have direct costs of substantial proportions for such agencies.⁸⁰ Such agencies could operate more effectively and more profitably without privacy regulation. Baycorp is in a semi-monopoly position in the credit reporting industry in New Zealand. Therefore, there is no financial incentive for Baycorp to develop a privacy culture in its organisation without being required to by legislation. For Baycorp, compliance with the Act is not a matter of good business practice. Leaving aside these few agencies, however this article will look at compliance costs faced by the majority of New Zealand businesses.

1 Establishment costs

Establishment costs are costs to modify existing structures, processes and training personnel whenever legislation is amended or new regulations are passed. The more frequently legislation is amended and the greater the scope of the amendments, the higher the costs will be to change existing systems and practices to comply with the new legislation. In general, one of the major establishment costs to an organisation is time spent understanding the legislation and how to comply with it.⁸¹ The more complex the legislation is, the more likely that an organisation will have to enlist professional assistance to understand how to meet its statutory obligations and, therefore, the higher the establishment costs.

⁸⁰ Recent regulation targeted to agencies in this sector is the Credit Reporting Privacy Code 2004.

⁸¹ *Finding the Balance*, above n 9, para 2.2.1.

Establishment costs can also be defined as those "one-off" costs incurred by new organisations. New businesses are constantly coming into existence and they are required to meet the costs of complying with the laws of the country in which they are incorporated. Such costs may be considerable and add materially to business start-up expenses and, therefore, can affect business viability.⁸²

Costs incurred to modify systems and processes to comply with new legislation can be minimised by providing a transition period. This can have the result of delaying and maybe preventing altogether the effect of high establishment costs. Rob Munro MP supported a transitional measure during the Bill's second reading when he stated that: "[the Bill] is being phased in to avoid disruption to business and to minimise compliance costs".⁸³

Another measure to phase in the requirements of the Act in order to minimise compliance costs and disruption to business was contained in section 8(4). This provided that nothing in Information Privacy Principle 3 applied to the collection of personal information on forms printed before the commencement of the Act as long as these forms were used before 1 July 1995.

Transitional provisions such as these are not generally available. Usually organisations are expected to comply with the legislation from the start. Additionally, new agencies do not have a lead-in time. They have to comply with the legislation from their first day of operation. At this stage of the agency's life cycle, compliance with privacy legislation is unlikely to be high on the list of priorities – especially where the agency is an individual rather than a company or other organisation.⁸⁴ Therefore, it is possible that the imposition of new legislation, having very little effect on the actions and behaviour of agencies, does not, in general, require transition periods to reduce compliance costs. While compliance costs will exist they will not be in the forefront of the agency's mind and the agency will develop systems and procedures to comply with the legislation.

2 *Ongoing costs*

The other type of direct business cost is the ongoing cost of complying with legislation. These are the focus of this article.

82 Business New Zealand survey response, above n 9.

83 Rob Munro MP (20 April 1993) 534 NZPD 14728. Another example is section 9(1) of the Act which provided for the postponement of the application of Information Privacy Principle 11 to direct marketing lists until 1 July 1996.

84 Definition of "agency" means "any person or body of persons, whether corporate or unincorporate ...": Privacy Act 1993, s 2(1). This article will use the terms "agency" and "organisation" interchangeably.

In general, ongoing compliance costs include:⁸⁵

- Time required to keep abreast of changes; and
- Time spent on paperwork, attending meetings, monitoring and demonstrating compliance and disseminating information.

As the saying goes, "time is money" and these ongoing compliance costs can impose a significant financial burden on many businesses, especially small enterprises. The 2004 Business NZ-KPMG *Compliance Cost Survey* found that small enterprises (those with five or fewer employees) bear substantial compliance costs of around \$2,750 per employee per year while large enterprises (those with over 100 employees) only face costs of around \$500 per employee per year.⁸⁶

Time spent on paperwork and demonstrating compliance may not actually be incurred by the organisation itself. Instead, the organisation may engage professional assistance such as through accountants or lawyers in order to achieve regulatory compliance. This represents a considerable cost to the organisation, especially for small to medium sized enterprises.

Specifically under the Act, the most widely cited ongoing business costs in my survey were:

- ensuring staff are aware of the Act's provisions and guidelines;⁸⁷
- dealing with access requests under the Act, including staff time in checking files and gathering the required information and then responding to requests;⁸⁸ and
- seeking legal advice when required.⁸⁹

These direct costs incurred by an organisation in complying with the Act are not the only costs included in the scope of the concept of "compliance costs". The compliance burden on an organisation can also include largely non-quantifiable and intangible costs.⁹⁰

⁸⁵ *Finding the Balance*, above n 9, para 2.2.1.

⁸⁶ *Business New Zealand-KPMG Compliance Cost Survey*, above n 5; Business New Zealand-KPMG "Small Firms Still Worst Hit by Compliance Costs" (26 August 2004) Media Release.

⁸⁷ Author's "Privacy Act 1993 Compliance Costs Survey" New Zealand Law Society response (21 June 2004).

⁸⁸ New Zealand Law Society survey response, above n 87; Author's "Privacy Act 1993 Compliance Costs Survey" Franklin District Council response (undated, returned July 2004).

⁸⁹ New Zealand Law Society survey response, above n 87.

B Non-Quantifiable and Intangible Costs

Non-quantifiable and intangible costs include mental stress and anxiety faced by businesses in complying with the ever changing regulatory obligations. They also include opportunity costs of time and resources used in ensuring compliance with the legislation that could be employed in more efficient and productive ways.⁹¹ These "psychic costs", as they are sometimes known, are often overlooked when considering the regulatory burden faced by organisations.⁹²

Legislation that provides large penalties for non-compliance or enactments that impose strict liability are likely to impose greater stress and anxiety on an organisation. For instance, tax legislation imposes very large penalties for non-compliance. Additionally, liability under this legislation is strict – organisations and individuals can be penalised even if they mistakenly or inadvertently file an incorrect tax return. Even where organisations enlist professional assistance to ensure compliance with taxation legislation, making sure that the correct information is given to these professionals may cause added levels of stress. It may be partly due to this level of stress and anxiety that taxation legislation is consistently cited as the enactment imposing the highest compliance costs on businesses.⁹³

As with any legislation that creates potential liability, the Privacy Act imposes stress and anxiety on agencies. For example, delays before complaints are investigated increases anxiety for agencies – particularly small enterprises. Although, sanctions for breach of the Act's provisions are very minor compared to those under taxation legislation they may not be insignificant.⁹⁴

C Not All Costs Imposed by Legislation are Compliance Costs

Whilst the concept of "compliance costs" is very broad, encompassing as it does both direct business costs and intangible and non-quantifiable costs, there are limitations on its breadth. Importantly, the concept is limited to those costs incidental to the regulatory

90 See for example, *Business Compliance Cost Statements*, above n 4, 6; *Finding the Balance*, above n 9, para 1.3; Sandford and Hasseldine, above n 36, 6.

91 *Business New Zealand-KPMG Compliance Cost Survey*, above n 5.

92 Sandford and Hasseldine, above n 36, 6.

93 See for example, *Red Tape Survey*, above n 5; Alexander, Bell and Knowles, above n 5; *Business New Zealand-KPMG Compliance Cost Survey*, above n 5; *Finding the Balance*, above n 9.

94 There are no sanctions under the Act during investigation. However, sanctions faced upon being found to have breached the Act are damages and court costs. Damages awards can be up to \$200,000 in the Human Rights Review Tribunal. The top award in the privacy area has been \$40,000 in *Hamilton v The Deanery 2000 Ltd* (29 August 2003) HRRT 36/02, Decision No 28/03.

obligation itself.⁹⁵ It does not extend to covering costs to a business such as the amount of tax paid or other substantive costs imposed by legislation.

Furthermore, it does not cover those costs that an organisation would incur in the absence of regulation. Many businesses have difficulty disentangling compliance costs from the business, tax and information handling activities that are a necessary part of running a business.⁹⁶ The Small Business Deregulation Task Force set up by the Australian Commonwealth Government stated that there is a degree of overlap between the practices a business will undertake in the absence of regulation and those that regulation requires them to do.⁹⁷ For example, privacy regulation requires firms to handle personal information in a particular way. When asked about the costs of complying with regulation, it is usual for an organisation to turn their mind to these costs. However, taking these costs as being the compliance costs imposed by legislation may not portray the true extent of the regulatory burden.⁹⁸ If firms would do many of the things that regulation obliges them to do, even in the absence of regulation, then these are not strictly "costs businesses incur when meeting a regulatory obligation".⁹⁹ Instead, "compliance costs" are those "incremental costs of compliance caused by regulation [rather than] the total cost of activities that happen to contribute to regulatory compliance."¹⁰⁰

Perceptions of the extent of the regulatory burden may be influenced by costs other than strictly "compliance costs". As mentioned previously in the context of Australian privacy legislation,¹⁰¹ some political decisions are made on the basis of perceptions rather than reality. Therefore, it is important to consider the factors that influence perceptions of compliance costs.

95 Ministry of Commerce *Compliance Cost Assessments and Statements: Guidelines for Departments* (Wellington, 1997) 7.

96 Ian Bickerdyke and Ralph Lattimore *Reducing the Regulatory Burden, Does Firm Size Matter?* (Industry Commission Staff Research Paper, Australian Government Publishing Service, Canberra, 1997) 10.

97 Charlie Bell *Time for Business Report of the Small Business Deregulation Task Force* (Report Number 037/96, Department of Industry, Science and Technology, Canberra, 1996) 15 as cited in Bickerdyke and Lattimore, above n 96, 10.

98 Europe Economics *Costs of Compliance: A Report by Europe Economics* (London, 2003) para 2.1 available at <<http://www.europe-economics.com>> (last accessed 10 October 2005).

99 Business New Zealand survey response, above n 9.

100 I Alton and P Andrews *Cost-Benefit Analysis in Financial Regulation: How to do it and How it Adds Value* (Financial Services Authority Occasional Paper Series 3, 1999) as cited in Europe Economics, above n 98, para 2.1.

101 See Part II C Australia.

D Non-Compliance Costs

Perceptions about the extent of "compliance costs" under the Act are likely to be influenced by many things. For example, the size of the organisation and the industry it operates in both contribute to the amount of personal information handled and therefore how much impact the Act has on everyday business practices. Additionally, the size of the costs associated with not complying with the legislation ("non-compliance costs") affect organisations' perceptions about the regulatory burden. Rather than bearing the compliance costs involved – such as appointing a privacy officer – organisations may "trade-off non-compliance with detection (and associated penalties)".¹⁰² Accordingly, these organisations will perceive the regulatory burden they face to be minimal. However, it is not advisable for governments to take these perceptions at face value and conclude that the regulatory burden is negligible. The particular enactment should be assessed to see whether it needs amendment to better achieve its stated objectives and encourage compliance.¹⁰³

Non-compliance costs can include formal penalties under the Act or informal sanctions experienced by an organisation when they neglect to fulfil their obligations under the Act. For example, these could take the form of "loss of business due to bad reputation/negative publicity".¹⁰⁴ One survey respondent indicated that non-compliance costs "due to negative publicity/reputation" were "far greater" than direct business compliance costs.¹⁰⁵

E Summary

There are a multitude of different costs that make up the concept of "compliance costs". It is useful to keep both the broad scope of this concept and its boundaries in mind when analysing compliance costs.

To illustrate the concept of compliance costs from an economic viewpoint, consider the following graph:¹⁰⁶

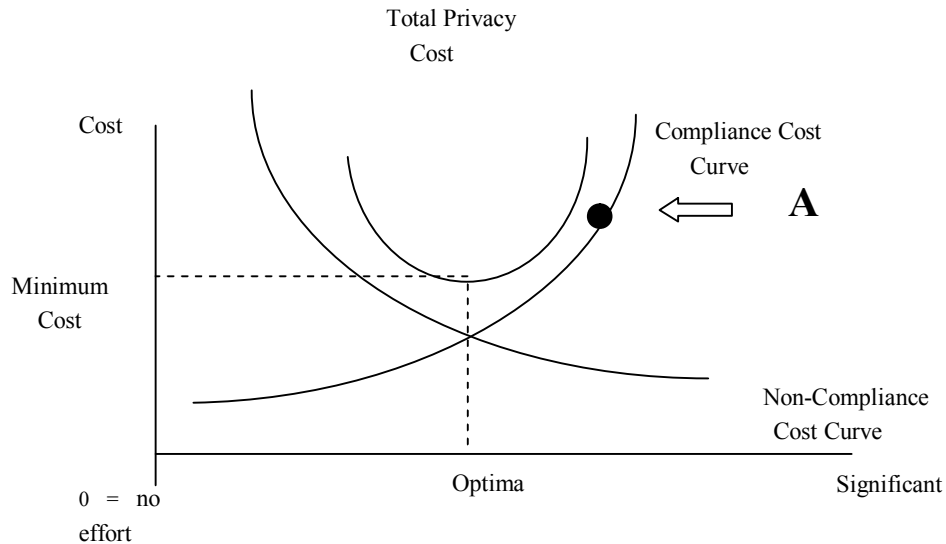
¹⁰² Bickerdyke and Lattimore, above n 96, 70-71.

¹⁰³ This is discussed in more detail below at Part IV C Privacy Officer Requirement.

¹⁰⁴ Author's "Privacy Act 1993: Compliance Costs Survey" Citigroup Auckland response (19 July 2004).

¹⁰⁵ Citigroup Auckland survey response, above n 104.

¹⁰⁶ Adapted from a total privacy cost framework graph in Dr Larry Ponemon, Chairman and Founder of Ponemon Institute "Trust and the Value of Privacy: Comments on Costs and Benefits" (Privacy and Data Security Academy and Expo, hosted by the International Association of Privacy Professionals, Chicago, 31 October 2003). The Ponemon Institute is "dedicated to advancing ethical information and privacy management practices in business and government. To achieve this objective, the Institute conducts independent research, educates leaders from the private and public



The graph shows that total privacy costs are the sum of compliance and non-compliance costs. There is a distinction drawn between "compliance" and "non-compliance" costs. The graph depicts the inherent trade-off between these two types of costs. It is optimal for businesses to put time and effort into complying with the Act up to the point where compliance costs are equal to non-compliance costs. This is where the total cost of privacy is at its lowest.

Consider an organisation putting time, effort and cost into complying with the Act at a level corresponding to point "A" on the graph. This organisation may have inefficient systems and processes in place to ensure compliance with the Act. This firm's total cost of privacy is higher than optimal, since non-compliance costs are lower than compliance costs at this point, the organisation would be better off not complying with the legislation. This organisation is likely to view the legislation as imposing high compliance costs. However, the fault is with the business' operations rather than the legislation itself. This organisation's perception may be different from the reality of the legislation. Consequently, perceptions should be viewed with caution. This highlights the need for empirical research to assess the actual regulatory burden.

Sometimes, despite organisations implementing efficient processes and systems, legislation still imposes higher than optimal total costs on them. The following section

sectors and verifies the privacy and data protection practices of organizations in a variety of industries": <<http://www.ponemon.org>> (last accessed 10 October 2005).

looks at specific instances of compliance costs under the Act and, in particular, suggests ways in which the Act could be amended to "minimise" these costs.

IV COMPLIANCE COSTS AND THE PRIVACY ACT 1993

A Background

The desire to minimise compliance costs was an "explicit consideration in the design of the Privacy Act 1993".¹⁰⁷ The Act does not impose licensing or registration requirements on businesses;¹⁰⁸ instead it gives businesses flexibility to choose how to meet their obligations under the Act.¹⁰⁹ Despite this, many organisations, particularly interest groups, made submissions regarding compliance costs to the Justice and Electoral Select Committee when this Committee was considering the Privacy of Information Bill 1991 (the Bill). Financial institutions were a particularly vocal group. The general tenor of their submissions was that the Bill, if enacted in its current form, would impose heavy compliance costs on banks and other credit providers.¹¹⁰ These submitters cited the Act's coverage of both the private and public sectors as the main reason for their concern about compliance costs. They argued that there needed to be a thorough analysis of the costs in extending the legislation to private sector organisations and that these costs should be balanced against the benefits.¹¹¹

Apart from minor changes,¹¹² the Select Committee decided against acting on financial institutions' concerns and did not derogate from the uniform coverage of both the public and private sectors.

¹⁰⁷ *Compliance Cost Submissions*, above n 12, introduction.

¹⁰⁸ This contrasts with the United Kingdom under the Data Protection Act 1998, Part III, which requires data controllers to notify the Data Protection Commissioner before they process any personal data and this has to be entered onto a register.

¹⁰⁹ *Discussion Paper 9*, above n 1, 6.

¹¹⁰ See, for example, Westpac Banking Corporation "Submission to the Justice and Law Reform Committee on the Privacy of Information Bill 1991"; ANZ "Submission to the Justice and Law Reform Committee on the Privacy of Information Bill 1991"; New Zealand Bankers' Association "Submission to the Justice and Law Reform Committee on the Privacy of Information Bill 1991".

¹¹¹ Westpac Banking Corporation "Submission to the Justice and Law Reform Committee on the Privacy of Information Bill 1991"; ANZ "Submission to the Justice and Law Reform Committee on the Privacy of Information Bill 1991"; New Zealand Bankers' Association "Submission to the Justice and Law Reform Committee on the Privacy of Information Bill 1991".

¹¹² For example, the Select Committee changed the charging regime: see discussion in Part IV B 1 Background.

The New Zealand Act still covers both the private and public sectors. If the financial institutions' initial concerns were valid, one would expect these organisations to respond to reviews and surveys about compliance costs and the Act in a negative way. That is, one would expect them to continue to argue that compliance costs under the Act are excessive. Interestingly, though, the submissions received in response to the Privacy Commissioner's *Discussion Paper* in 1998 and the results of my questionnaire last year, show that financial institutions appear to have no major concerns about compliance costs under the Act. Indeed, two respondents to my survey suggested that customers demand privacy and that procedures in place to protect privacy were a matter of good business practice, which they would maintain without the Act mandating such practices.¹¹³ These respondents also stated that nothing more could be done under the Act to minimise compliance costs.¹¹⁴ This evidence demonstrates how perceptions of compliance costs can be different to actual reality. The results of the Privacy Commissioner's review of the Act and my survey show that the benefit of having uniform privacy protection across both the public and private sectors does not seem to have accrued at the expense of higher compliance costs to businesses.

Even though the Act sought to minimise the regulatory burden as much as possible, it is worthwhile to periodically assess whether it is still achieving this aim in practice. Particularly given that the Commissioner is required to have regard to the "general desirability of a free flow of information and the recognition of the right of government and business to achieve their objectives in an efficient way".¹¹⁵

In the 1997-1998 review of the Act, two aims of the Commissioner were to examine "various features which contribute to the low compliance costs imposed by the Act" as well as attempt to determine "whether it would be possible through amendment ... to improve the position even further with respect to compliance costs".¹¹⁶ The recommendations made to "reduce" compliance costs were to:

- prohibit private sector agencies from charging for the correction of information in response to an information privacy request;¹¹⁷

113 Citigroup Auckland survey response, above n 104; Author's "Privacy Act 1993 Compliance Costs Survey" Kiwibank Limited response (via telephone, 14 July 2004).

114 Kiwibank Limited survey response, above n 113; Citigroup Auckland survey response, above n 104.

115 Privacy Act 1993, s 14(a).

116 *Necessary and Desirable*, above n 7, 7.

117 *Necessary and Desirable*, above n 7, paras 5.4.4-5.4.6 (recommendation 65).

- amend section 7 (savings provision) to enhance privacy rights while simplifying the position at the same time;¹¹⁸ and
- redraft the charging provisions to make them more understandable.¹¹⁹

The next sections of this article discuss some of the specific compliance costs imposed by the Act, keeping in mind the above recommendations to come out of *Necessary and Desirable* (the report outlining the findings of the 1997-1998 review of the Act). The article will suggest additional ways in which the Act could be amended to minimise these costs. An analysis of the costs and benefits of each amendment will be attempted. The focus will be on two of the largest direct business costs associated with complying with the Act. Specifically, these are costs incurred by an organisation in processing and complying with an information privacy request and costs expended in meeting the requirement to have at least one privacy officer under section 23 of the Act.

B Charging Regime

1 Background

Before the Privacy Act was enacted, the OIA governed access to both personal and "official information" held by public sector agencies.¹²⁰ There was no equivalent legislation regulating personal information held by private sector agencies. The general presumption underlying the OIA is to "make official information more freely available"¹²¹ unless an exception applies.¹²² In accordance with this purpose, under the OIA, agencies could recover costs incurred in complying with access and correction requests relating to official information,¹²³ but they were prohibited from charging for requests for access and correction of personal information.¹²⁴ Charging for access to official information against this background does not appear to have detracted from these purposes; that is, people still make requests even though they have to reimburse reasonable costs incurred by an agency in

¹¹⁸ *Necessary and Desirable*, above n 7, para 2.15.13.

¹¹⁹ *Necessary and Desirable*, above n 7, paras 5.4.1-5.4.3 (recommendation 64).

¹²⁰ Official Information Act 1982, s 24 (in force from 1 April 1987 to 30 June 1993) governed the right of access to personal information; Official Information Act 1982, s 21 governed the right of access to certain official information.

¹²¹ Official Information Act 1982, Long Title.

¹²² Official Information Act 1982, s 5.

¹²³ Official Information Act 1982, s 15(1) and (2).

¹²⁴ Official Information Act 1982 s 24(1) (in force from 1 April 1987 to 30 June 1993) stated: "... every person has a right to and shall, on request, be given (*in the case of a natural person, without charge*) access to any personal information ..." (emphasis added).

meeting their request. There does not appear to have been a lessening of public sector accountability merely because agencies can recover costs for official information access requests.

The original Privacy of Information Bill 1991 (the Bill) removed the provisions governing "personal information" from the OIA into a separate piece of legislation covering both public and private sector agencies. The OIA continues to govern access by a company to information about it held by public sector agencies¹²⁵ and access to "official information" about third parties held by public sector agencies.¹²⁶ The Bill as introduced did not allow *any agency* to charge for giving an individual access to his or her personal information.¹²⁷ By way of exception to this general rule, clause 35(2) of the Bill provided that public sector agencies could charge for making information available in accordance with the proposed Principle 8. Principle 8 provided that an individual was entitled to request reasons for decisions made in respect of that individual by certain *public sector agencies* within a reasonable time of the making of the decision. This Principle was directly imported from section 23 of the OIA.

The renamed Privacy Bill as reported back from the Justice and Law Reform Select Committee omitted clause 35 as discussed above (as well as deleting Principle 8) and replaced it with the current section 35 in the Act. Broadly, this section only allows *private sector* agencies to recover costs incurred in making information available in compliance with an access or correction request. Public sector agencies cannot charge as a general rule.¹²⁸ The reason for this turnaround is less than clear given the absence of a formal report from the Select Committee and no detailed Parliamentary debate on this issue.

One possible reason is that the Select Committee decided to maintain the status quo in regards to charging individuals for accessing their own personal information as provided in the previous OIA.¹²⁹ Public sector agencies had previously absorbed the costs of individuals accessing their own personal information under the OIA and the Select Committee may not have seen any good reason to alter this. This provides an explanation for why public sector agencies are not permitted to charge under the Act. However, it does not explain why private sector agencies have been given the right to charge in some circumstances.

125 Official Information Act 1982, Part 4.

126 Official Information Act 1982, Part 2.

127 Privacy of Information Bill 1991, no 84-1, cl 35(1).

128 The current charging regime is elaborated on in Part III B Current Charging Regime.

129 Official Information Act 1982 s 24(1) (in force from 1 April 1987 to 30 June 1993).

A possible explanation as to why private sector agencies were given the right to charge is due to public pressure through the submissions process regarding the private sector coverage of the Act. A majority of submissions cited the excessive compliance costs that would be imposed by the Act on private sector agencies and the non-applicability of many provisions to the private sector as reasons that the Act should not cover this sector.¹³⁰ Therefore it may have been partly to appease this majority of submitters who argued against the Bill's coverage of the private sector that the Select Committee allowed private sector agencies to charge for making information available pursuant to access and correction requests in the final draft of the Bill. There was no written Select Committee Report produced in relation to the Bill, so we do not know the actual reasons for the Select Committee's decision to allow private sector agencies to charge.

Another reason why the Select Committee may have changed the charging regime was because the Bill marked the first time private sector agencies had been subject to privacy legislation. Therefore, it was difficult to estimate the expected costs faced by private sector agencies under the new legislation. These costs were known for public sector agencies under the previous OIA regime but it was unknown whether such costs would be a good proxy for what was likely to happen in the private sector once the legislation was enacted. Potentially private sector agencies could have faced a much greater number of requests and, at least initially, may have experienced far greater costs than public sector agencies due to their inexperience in dealing with these requests. For these reasons, the Select Committee may have taken a cautious approach and allowed private sector agencies to charge for "information privacy requests". If subsequent research once the Act was enacted showed that there was little practical difference in costs faced by public and private sector agencies and, therefore, the distinction drawn in the charging regime was without basis, then the Act provided for a periodic review under section 26 so this could be corrected.

2 *Current charging regime*

The provisions relating to charges are located in Part 5 of the Act. Section 33 prescribes the application of Part 5 of the Act. It states:¹³¹

This Part applies to the following requests (in this Act referred to as information privacy requests):

¹³⁰ See for example, Westpac Banking Corporation "Submission to the Justice and Law Reform Committee on the Privacy of Information Bill 1991"; ANZ "Submission to the Justice and Law Reform Committee on the Privacy of Information Bill 1991"; New Zealand Bankers' Association "Submission to the Justice and Law Reform Committee on the Privacy of Information Bill 1991".

¹³¹ Privacy Act 1993, s 33 (emphasis omitted).

- (a) a request made pursuant to subclause (1)(a) of principle 6 to obtain confirmation of whether or not an agency holds personal information:
- (b) a request made pursuant to subclause (1)(b) of principle 6 to be given access to personal information:
- (c) a request made pursuant to subclause (1) of principle 7 for correction of personal information.

In other words, the charging provisions apply to "information privacy requests".

Public sector agencies have a limited right to apply to the Commissioner for authority to recover costs incurred in making information available in compliance with an access or correction request.¹³² The Commissioner may grant such authority where he or she is satisfied that the public sector agency is "commercially disadvantaged in comparison with any competitor in the private sector, by reason that the agency is prevented ... from imposing a charge".¹³³ For most public sector agencies this will be nearly impossible to show because they do not have private sector counterparts.¹³⁴

In contrast, private sector agencies are automatically allowed to require payment for some costs incurred in making information available in compliance with an access or correction request.¹³⁵ Such charge must be "reasonable" and, when determining reasonableness, regard may be had to the costs of the labour and materials involved in making the information available to the applicant or to additional costs incurred where the applicant has requested the application be treated as urgent.¹³⁶ Disputes about the reasonableness of charges imposed are to be investigated and adjudicated on by the Commissioner.

132 Privacy Act 1993, s 35(1).

133 Privacy Act 1993, s 36(1).

134 For instance, the Ministry of Education and the Police have major costs associated with granting access to personal information: Author's "Privacy Act 1993 Compliance Costs Survey" Ministry of Education response (24 June 2004) regarding the costs of granting access to personal information faced by Ministry of Education; and Office of the Privacy Commissioner *Annual Report of the Privacy Commissioner for the Year Ended 30 June 2003* (Wellington, 2003) 28 [*Annual Report of the Privacy Commissioner for the Year Ended 30 June 2003*] for the comment that the Police are large repositories of personal information, which implies large costs associated with granting access to personal information. However, these agencies have no private sector competitors. Therefore it will be extremely difficult for these agencies to prove that they are at a commercial disadvantage by reason of the operation of the charging regime under the Privacy Act 1993.

135 Privacy Act 1993, s 35(3).

136 Privacy Act 1993, s 35(5).

In practice, there is evidence that private sector agencies choose not to charge for small requests because the paperwork involved in invoicing an individual outweighs the costs recovered. Only one bank, Westpac, expressly details costs associated with information privacy requests on their website. They charge five cents per page for photocopying plus \$20 an hour and there is no charge if the copying is less than 50 pages. This practice of not charging for small requests, however, is not binding under the Privacy Act in contrast to the OIA.

The practice under the OIA is governed by the *Charging Guidelines for Official Information Act 1982 Requests*¹³⁷ the most recent version of which was issued by the Ministry of Justice in March 2002. These *Guidelines* should be followed for all requests under the OIA unless good reason exists for not doing so.¹³⁸ They outline how charges should be set and what are reasonable levels. While not binding on information privacy requests under the Privacy Act, they provide some guidance to private sector agencies as to what are likely to be "reasonable charges" under the Privacy Act. For example, the *Guidelines* provide that staff time incurred in processing a request under the OIA should only be charged after the first hour at a rate of \$38 per half hour.¹³⁹ Additionally, photocopying or printing is charged at 20 cents per page, with the first 20 pages free.¹⁴⁰

Under the Privacy Act, private and public sector agencies alike are prohibited from charging for any costs incurred with helping an individual make a request for information, transferring the request to another agency or processing the request and deciding whether it should be granted or not.¹⁴¹ In other words, section 35 draws a fine distinction between, on the one hand, making information available pursuant to an information privacy request and,

137 Ministry of Justice *Charging Guidelines for Official Information Act 1982 Requests* (Wellington 2002). [*Charging Guidelines for Official Information Act 1982 Requests*].

138 *Charging Guidelines for Official Information Act 1982 Requests*, above n 137, 1.

139 *Charging Guidelines for Official Information Act 1982 Requests*, above n 137, 3.

140 *Charging Guidelines for Official Information Act 1982 Requests*, above n 137, 4. This article argues that this charge is not "reasonable" and should not be used as a guide by private sector agencies looking to impose "reasonable" charges under the Privacy Act 1993. A ream of paper (500 sheets) costs approximately \$10.00, which equates to less than 2 cents a page. Adding on costs for toner or ink, which are no more than 7 cents per page (information from the Hewlett Packard website based on LaserJet printers, which are common amongst businesses: <<http://www.hewlettpackard.com>> (last accessed 10 October 2005)), the actual total cost per page would be less than 10 cents. The author suggests that a charge of 10 cents per page for photocopying and printing is more "reasonable". This charge is supported by organisations such as Victoria University of Wellington who charge 10 cents per page for photocopying and printing facilities used by its students. Agencies should not be attempting to make a profit under this charging regime.

141 Privacy Act 1993, s 35(2).

on the other hand, the making of the request, transfer of the request to another agency, processing of the request or the provision of assistance. In practice, it is likely to be difficult for laypeople to know exactly what they are permitted to charge for and what they are not. As recommended in *Necessary and Desirable*, this section needs to be redrafted to set out clearly what private sector agencies can charge for and to provide a list of all the charges that public sector agencies are prohibited from passing on.¹⁴²

Arguably, it is inequitable that private sector agencies should be able to charge under the Privacy Act whilst public sector ones cannot.¹⁴³ The sector an agency operates in has no effect on the amount of costs incurred in making information available under an access request or correcting information pursuant to a request. If a request requires an agency to undertake a time-consuming search through archived and other historical files, there should not be a different rule regarding cost recovery depending on which sector the agency is operating in. An arbitrary distinction based on the sector the agency operates in is anomalous in the current business environment given that the line between what is a public sector organisation and what is a private sector organisation has been increasingly difficult to draw, for example since the mid 1980's when the number of state owned enterprises increased.¹⁴⁴

If this policy distinction is elusive, section 35 should be amended to provide a level playing field for agencies. Accordingly, the Privacy Act needs to either extend the charging regime to include public sector agencies or to prohibit charging by *any* agency. The next section will consider which of these options is most feasible both from a compliance cost perspective and from a privacy point of view.

3 *Should all agencies be permitted to charge or should the Act prohibit charging by all agencies?*

Most organisations that responded to my survey suggested that the current cost recovery regime provided for in section 35 of the Act was adequate. However, two organisations argued that the right to charge should be extended to public sector agencies.¹⁴⁵

Undoubtedly any movement towards permitting all agencies to charge under section 35 would reduce compliance costs under the Act. However, compliance costs cannot be looked

142 *Necessary and Desirable*, above n 7, paras 5.4.1-5.4.3.

143 *Compliance Cost Submissions*, above n 12, FinSec submission WX1 (14 October 1997).

144 Geoffrey Palmer and Matthew Palmer *Bridled Power: New Zealand's Constitution and Government* (4 ed, Oxford University Press, Melbourne, 2004) 96 and 111.

145 Ministry of Education survey response, above n 134; and, interestingly, Business New Zealand survey response, above n 79.

at in isolation.¹⁴⁶ There are limits to the extent to which the regulatory burden can be reduced.¹⁴⁷ The Privacy Commissioner cautions against any moves to reduce compliance costs that come at the expense of protecting privacy under the Act.¹⁴⁸

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.

A balance needs to be struck between minimising compliance costs for organisations and protecting individuals' privacy. In other words, any charging regime imposed under the Act must ensure that information privacy requests by individuals are not inhibited. This would be contrary to the spirit of the Act. The Privacy Act provides that individuals have a right to access and correct their personal information unless there is good reason to prevent them from doing so.¹⁴⁹ The major purpose of the Act is to "promote and protect privacy".¹⁵⁰ Arguably, requiring individuals to pay for information privacy requests considerably weakens the force of this right and is contrary to the spirit and intention of the Act. Individuals should not have to pay to protect their privacy.¹⁵¹

(a) Charging for correction

The argument that individuals should not have to pay to protect their privacy is further strengthened when considering the application of the charging regime to correction requests. Critics of the ability to charge see it as objectionable that an agency should be permitted to charge an individual for the "privilege" of correcting their personal information held by the agency.¹⁵² It seems incongruous that if an individual asks a third party to request a correction of the individual's personal information on their behalf the agency cannot pass on the costs of correction, but if this individual makes the request himself or herself, he or she

146 *Compliance Cost Submissions*, above n 12, 4.

147 Bickerdyke and Lattimore, above n 96, 13.

148 *Compliance Cost Submissions*, above n 12, 4.

149 Privacy Act 1993, Information Privacy Principle 6; subject to the provisions in Privacy Act 1993, Parts 4 and 5.

150 Privacy Act 1993, Long Title.

151 For example, in relation to telecommunications and privacy law the recent Telecommunications Information Privacy Code 2003, Schedule 3 cl (1)(e) provides that individuals must be able to obtain per-line caller identification blocking of their number for telephone calls they make and the means to obtain per-call blocking as well as to ascertain whether an outgoing line is blocked, free of charge. In other words, individuals should not have to pay to maintain their privacy.

152 *Necessary and Desirable*, above n 7, para 5.4.4.

is exposed to possible expense recovery by the agency.¹⁵³ Indeed, under principle 7(2), agencies are required to take reasonable steps to correct personal information to ensure that it is up to date, complete and not misleading. It is anomalous to have a provision for charging individuals to correct information where the Act also provides in Principle 8 that the accuracy of personal information is to be checked before use. The Rt Hon David Lange MP recognised this anomaly during the second reading of the Bill when he said:¹⁵⁴ "I suggest that it is contrary to the spirit of the Bill itself that there should be a charge made when the law requires the person holding the information to have it correct".

When an individual makes a correction request relating to their personal information, not only does this person receive a benefit, but society also gains from the agency holding accurate personal information and having agencies make decisions based on up to date and relevant information. For this reason, it is not appropriate to make an individual bear the cost of the correction request.

These factors indicate that the application of the charging regime to correction requests is inappropriate and does not accord with the spirit of the Act. This paper supports the recommendation made by the Commissioner in his 1998 Review to repeal the application of the charging regime to correction requests made to private sector agencies.¹⁵⁵ In practice, this amendment is likely to have little negative effect on compliance costs for agencies because, as the Commissioner acknowledges,¹⁵⁶ charges for correction requests are hardly ever made.

(b) Charging for access

As part of their submissions to *Discussion Paper 9*, FinSec¹⁵⁷ stated that they had "had examples where cost has been a significant disincentive to employees accessing information held about them".¹⁵⁸ If this is a widespread experience under the Act, then amending the Act to permit all agencies to charge would inhibit legitimate requests for access. This is not in the best interests of society from a privacy point of view even though it does reduce compliance costs to agencies.

153 *Necessary and Desirable*, above n 7, para 5.4.5.

154 Rt Hon David Lange MP (20 April 1993) 534 NZPD 14726.

155 *Necessary and Desirable*, above n 7, para 5.4.6 (recommendation 65).

156 *Necessary and Desirable*, above n 7, para 5.4.6.

157 FinSec stands for the Finance Sector Union and in 1997 represented approximately 15,000 members working primarily in the New Zealand Banking and Insurance industries.

158 *Compliance Cost Submissions*, above n 12, FinSec submission WX1 (14 October 1997).

Individuals making requests for their own personal information under the Act provide benefits by ensuring that the organisation is accountable to individuals and allows individuals to maintain control over their personal information, which is an important foundation on which the Act is based.¹⁵⁹ These two factors are important in a free and democratic society, not only for the individuals concerned but also for the community at large. Therefore, based on similar arguments made in regards to correction requests, because society gets the ultimate benefit from the workings of the Act it should bear at least some of the compliance costs of organisations. Based on this reasoning, the current charging regime in the Act should be repealed and all agencies should be made to absorb these costs just as they do other business expenses. These compliance costs "are likely to be factored into the sale price of goods and services".¹⁶⁰ Society may be willing to pay a little bit more for goods and services it receives the benefit of greater protection of personal information. The costs of information privacy requests would be spread among a large number of consumers (or taxpayers in the case of a public sector agency), meaning that any one individual is only bearing a very small proportion of the cost compared with one individual requester shouldering the whole of the cost under the current regime. However, it is acknowledged this may have the effect of making the prices of goods and services provided by small businesses less competitive because small businesses are less likely to be able to absorb such costs, in comparison to large firms.

Compliance costs may be minimised for all agencies by amending Information Privacy Principle 6 to require individuals requesting access to their personal information to assist the agency by making a request with due particularity.¹⁶¹

Critics of the charging regime argue that it is not appropriate for public sector agencies to charge for access requests. Public sector agencies, in particular (although not exclusively), hold information at the requirement of an enactment leaving the individual little choice about whether to provide such information or not.¹⁶² Therefore, it would be

159 The Act was drafted in accordance with the Recommendation of the Council of the Organisation for Economic Co-operation and Development Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data: Privacy Act 1993, Long Title. Two principles contained in these Guidelines are the accountability principle as well as the individual participation principle: Organisation for Economic Co-operation and Development *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD, Paris, 2001) 16. The second of these principles ensures an individual maintains control of their personal information.

160 Business Professional Services Limited survey response, above n 8.

161 Author's "Privacy Act 1993 Compliance Costs Survey" Victoria University of Wellington response (15 July 2004). Precedent can be found in the OIA where official information requested shall be specified with due particularity: Official Information Act 1982, s 12(2).

162 Franklin District Council survey response, above n 88.

unreasonable to ask the individual to pay to access their personal information where they have provided it pursuant to the coercive power of the state.¹⁶³ An access request not only includes actual access to an individual's personal information held by the agency, but also extends to obtaining confirmation as to whether or not the agency holds certain personal information, which is a necessary precursor to correction requests.¹⁶⁴ It is important that agencies collecting personal information coercively from individuals are accountable for what information they hold. An access request is the first step in holding an agency accountable. Given the fundamental importance placed on accountability in modern societies, it is inappropriate for an individual to have to pay to uphold this principle.¹⁶⁵

4 Charging guidelines

If charging were to be kept, this paper supports the creation of charging guidelines under the Act similar to those issued by the Ministry of Justice under the OIA.¹⁶⁶ It is preferable that any guidelines issued by the Commissioner are consistent with those issued under the OIA.¹⁶⁷ Certainty of costs is an important concept in the business world. Guidelines must be flexible enough to apply to any situation that arises while at the same time providing certainty to requesters and agencies alike.¹⁶⁸

As part of the 1998 Review of the Act, the Commissioner specifically canvassed the possibility of creating charging guidelines.¹⁶⁹ Most submitters supported the notion of guidelines.¹⁷⁰ Those opposed to the idea were concerned that the guidelines might be overly restrictive or too inflexible.¹⁷¹

163 Franklin District Council survey response, above n 88.

164 Privacy Act 1993, Information Privacy Principle 6(1)(a) and (b).

165 The Danks' Committee set up to look at official information, summed up the opposing arguments in this way: "any system of charging is likely to be challenged by those who see ability to pay as imposing an unreasonable constraint on a democratic entitlement. But a "free" system of access would be a blank cheque for the use of public resources": Committee on Official Information (Danks' Committee) *Towards Open Government: Supplementary Report* (Volume 2, Wellington, 1981) 35.

166 See Part IV 2 Current charging regime.

167 *Necessary and Desirable*, above n 7, 188 quoting New Zealand Bankers' Association submission S25 (date not cited).

168 *Necessary and Desirable*, above n 7, paras 5.4.20-5.4.21.

169 *Necessary and Desirable*, above n 13, para 5.4.20.

170 *Necessary and Desirable*, above n 13, para 5.4.21 footnote 47.

171 *Necessary and Desirable*, above n 7, para 5.4.21.

Accordingly, the Commissioner envisioned guidelines specifying that if a charge were to be made within a specified formula it would be presumed to be "reasonable".¹⁷² Charges exceeding or outside the formula would have to be shown to be reasonable in the event of a complaint.¹⁷³ This would ensure that the guidelines were flexible and adaptable enough to cover any circumstances that may arise.

The Commissioner currently has the ability to issue charging guidelines by invoking the power provided under section 46(4)(b). However, the former Commissioner, Bruce Slane, did not consider it a priority to issue such guidelines because he considered charging complaints to be so infrequent that issues surrounding "reasonableness" were more illusory than real.¹⁷⁴ He also considered that issuing guidelines might encourage agencies to charge.

In summary, if the current charging regime is maintained, this article supports written guidelines outlining what are "reasonable" charges under section 35 of the Act to minimise costs incurred by businesses and individuals due to uncertainty.

5 Summary

While prohibiting all agencies from charging for information privacy requests would increase compliance costs associated with the Act, such amendment would be unlikely to impose excessive compliance costs on agencies. The charging regime has been viewed as a significant disincentive to individuals requesting access to their personal information held by an agency.¹⁷⁵ Based on this, one may expect to see an increase in information privacy requests following a removal of the charging regime. The resulting benefit is that agencies will hold more accurate personal information and make decisions based on up to date and relevant information. Also, agencies will be more accountable for the personal information that they hold.

A cost-benefit analysis of this recommendation shows that there are clear benefits from removing the charging regime from the Act rather than maintaining the current regime and issuing charging guidelines. Such an amendment accords more with the spirit of the Act because it gives individuals more control over their personal information. However, it does increase compliance costs faced by agencies – especially private sector agencies who currently do not have to absorb all costs associated with information privacy requests. This increase in compliance costs is entirely justifiable from a privacy protection viewpoint.

172 *Necessary and Desirable*, above n 7, para 5.4.21 footnote 48.

173 *Necessary and Desirable*, above n 7, para 5.4.21 footnote 48.

174 *Necessary and Desirable*, above n 7, para 5.4.22.

175 *Compliance Cost Submissions*, above n 12, FinSec submission WX1 (14 October 1997).

Since this amendment would provide an overall net benefit to society, from an economic perspective, it cannot be argued that the increase in compliance costs is "excessive".

C Privacy Officer Requirement

Another potentially substantial business cost associated with complying with the Act is the requirement to appoint at least one person who is responsible for all the agency's privacy matters under the Act. Section 23 states:

It shall be the responsibility of each agency to ensure that there are, within that agency, 1 or more individuals whose responsibilities include –

- (a) the encouragement of compliance, by the agency, with the information privacy principles:
- (b) dealing with requests made to the agency pursuant to this Act:
- (c) working with the Commissioner in relation to investigations conducted pursuant to Part 8 in relation to the agency:
- (d) otherwise ensuring compliance by the agency with the provisions of the Act.

This is one of the few sections of the Act that is prescriptive in regards to methods of compliance. Compliance with this section increases agencies' costs in the short term. First, there are direct business costs incurred by agencies who comply with this section. One cost is initially training the privacy officer to know the requirements of the Information Privacy Principles and other provisions of the Act. The higher the turnover rate of employees in the position of privacy officer, the greater these initial training costs will be to an organisation.

There is also an ongoing cost to ensure that the privacy officer is continually educated on developments in information privacy law and how these changes apply to the particular agency.

Other costs are incurred by the privacy officer fulfilling their obligations under section 23. In ensuring compliance by the agency with the provisions of the Act, it is likely that the privacy officer will incur further ongoing compliance costs on behalf of the organisation. Specifically, the privacy officer needs to ensure that all staff are aware as to how information should be handled and collected in accordance with the Act. This includes development and awareness of internal controls and policies regarding handling and collecting personal information. These represent other ongoing costs to an organisation because when new staff are employed they need to receive training in internal policies associated with handling personal information.

Secondly, the privacy officer is commonly employed by the organisation in another capacity and his or her privacy officer obligations under the Act are only a very minor part

of the person's job description. There is an opportunity cost to the organisation when the privacy officer fulfils his or her obligations under the Act because by doing so he or she is unable to use this time to carry out their other responsibilities within the organisation. As long as the privacy officer's responsibilities under the Act are kept to a minimum and only extend to those necessary to achieve the purpose of the Act, then compliance costs will be minimised.

While there are certainly positive compliance costs, it can be argued that the provision of a privacy officer within an organisation actually *reduces* compliance costs for an agency. One respondent to my survey felt that costs associated with having at least one privacy officer in an agency added value to the business and potentially reduced the need to incur future compliance costs.¹⁷⁶ This respondent argued that a "properly trained and informed" privacy officer is a "prerequisite to ensure compliance in the first instance and the speedy resolution of complaints".¹⁷⁷ Having a dedicated person within an organisation dealing with privacy matters saves time and money when an access request or a complaint against the agency is made because this person is trained to deal with these matters in accordance with the Act.¹⁷⁸

Another reason that having a privacy officer can save an agency money in the long term relates to the collection and handling of personal information. With the help of a privacy officer, an agency can minimise its costs by putting in place collection procedures in compliance with the collection principles in the Act and implementing systems and policies that recognise the agency's obligations under the Act.¹⁷⁹ Where an agency's collection and handling procedures are in compliance with the Act, this agency is less likely to have a complaint made against it. Additionally, if the agency routinely makes personal information available proactively and is transparent about its handling and storage of personal information it is likely to ward off many complaints. A privacy officer is instrumental in encouraging agency compliance with these principles and encouraging an agency to equip people with information before they ask for it. Even though this requires an agency to spend money upfront on complying with the Act, costs will be saved in the long run from fewer complaints.

176 Business Professional Services Limited survey response, above n 8.

177 Business Professional Services Limited survey response, above n 8.

178 Additionally, training staff in relation to their obligations under the Act alerts them to their rights under the Act (*Compliance Costs Submissions*, above n 12, Franklin District Council submission WX2 (6 October 1997)), which can reduce compliance costs for that and other agencies. Privacy officers can educate family and friends on their rights under the Act and help foster a privacy culture.

179 Privacy Act 1993, Information Privacy Principles 1-4.

Given these potential benefits, and the requirements of the Act, I was surprised at the apparent lack of compliance with section 23, that I experienced in conducting my survey.¹⁸⁰

1 *Survey findings*

I phoned many of the organisations to speak to their "privacy officer" in regard to my survey. In almost every case the receptionist who answered my call did not know who the privacy officer of their organisation was. I thought the reason may have been because I used the title "privacy officer" and in most organisations (even large ones) the privacy officer has responsibilities other than their obligations under the Act. Therefore, this person may instead have been known by the title associated with their other responsibilities, such as "national compliance manager". However, even when I explained that I wanted to speak with the person in the organisation who deals with "your organisation's privacy matters" many receptionists were still unclear as to whom they should direct my call. This is a matter of concern. It must be an inefficient and time-consuming process for the Commissioner to locate the "privacy officer" within an agency where there is a complaint and the Commissioner has to investigate. Apparently, the Privacy Commissioner's practice is to contact the Chief Executive Officer (CEO) of the organisation in the first instance.¹⁸¹ The CEO will then pass on the information to the privacy officer if the organisation has one. This seems to be an inefficient way of handling communication between the Commissioner and an organisation. It would be much more expedient if the Commissioner had an up to date list privacy officers for each organisation in the country and contacted these people directly in relation to matters concerning privacy matters.

Additionally, and more importantly, this lack of compliance with section 23 of the Act causes problems for individuals requesting access to their information under the Act. Where, as is common, individuals decide to request access to their personal information initially by going directly to the organisation, they are likely to have difficulties getting hold of the appropriate person within the organisation to deal with their request.¹⁸²

180 The findings of my survey in regards to lack of compliance with section 23 are supported by a study of Australian businesses prepared for the Office of the Federal Privacy Commissioner in July 2001: Roy Morgan Research *Privacy and Business* (report for the Office of the Federal Privacy Commissioner, Sydney, July 2001) [*Privacy and Business*]. In response to the question "does your organisation have a nominated staff member to oversee privacy issues relating to the collection, transfer and use of customers' personal information?" 60 per cent of Australian businesses answered "no": *Privacy and Business*, above, 24.

181 Katrine Evans, Assistant Privacy Commissioner (Legal), to the author "Privacy Commissioner's Practice in Communicating with Agencies" (21 September 2004) Oral Conversation.

182 There is no requirement in the Privacy Act 1993 that a request be made in writing, nor that an individual go directly to the agency concerned first. Under section 68(1) of the Privacy Act 1993, a complaint to the Commissioner may initially be made either orally or in writing. Therefore,

Another concern resulting from my survey was the lack of understanding by respondents about the role of the privacy officer and the requirement for agencies to have one or more people who assume these responsibilities. One respondent stated that "every firm above a certain size (9 plus employees) should have a staff member acting as privacy officer".¹⁸³ It is encouraging that this firm understood the concept of a privacy officer. However, it is of some concern that they thought that only medium and large sized agencies needed to have a staff member acting as privacy officer. This response is incorrect, as the Act requires *all* organisations to have at least one staff member acting as privacy officer.¹⁸⁴

Given the lack of compliance with section 23 of the Act, one must consider what an appropriate response is. The Act does not provide penalties for non-compliance with this section. The Ministerial Panel on Business Compliance Costs' study showed that small businesses felt that there was no need for them to have a privacy officer due to the high cost of training staff on the requirements of the Act with no measurable benefit.¹⁸⁵ Faced with a raft of legislation all requiring action and with consequent compliance costs, organisations are likely to choose to comply with those enactments that provide the greatest penalty for non-compliance. By not providing penalties for non-compliance with this section, the Act provides no incentive to comply with the requirement to have a privacy officer.

It is clear that a response of some sort is needed to address this widespread non-compliance with section 23.

2 Options for reform

There are two possible solutions to address agencies' non-compliance with section 23. Either this section can be repealed because it is meaningless to have a legislative requirement that has low compliance and no penalties for non-compliance, or the Act could be amended to make it an offence for an agency not to have a privacy officer and provide consequent penalties. Of course it is one thing to have a privacy officer in name but it is another to ensure that this person fulfils the obligations set out in the Act. The penalty regime would have to be comprehensive enough to cover both forms of non-compliance.

(a) Repeal of section 23

because there is no specific requirement for a request to be made in writing initially, by analogy with section 68(1), arguably a request can be initially made orally. Accordingly, it is conceivable that an individual's first attempt to contact the agency with a request for access will be via telephone (where an individual decides to deal directly with the agency concerned in the first instance).

¹⁸³ Business Professional Services Limited survey response, above n 8.

¹⁸⁴ Privacy Act 1993, s 23.

¹⁸⁵ *Finding the Balance*, above n 9, para 6.8.3.

If the requirement to have a privacy officer were removed from the Act completely, compliance costs under this section would disappear. However, this is not the best response from a privacy protection viewpoint. Repealing this section would mean that there would be no requirement for an agency to have a person fulfilling the obligations set out in section 23. There would be no single person whose responsibilities were to ensure the agency's compliance with the Act's provisions. Without the privacy officer regime extra costs would be imposed on the Commissioner's office to ensure agencies complied with the Act and to undertake more extensive education about obligations under the Act. Therefore, it is more likely that compliance with the Act would be overlooked by many agencies.

This concern has not been the reality under the OIA. The OIA does not contain a corresponding duty on public sector agencies to appoint officers with similar responsibilities and there is no evidence that compliance with the OIA is being overlooked because of this. However, the experience under the OIA is not a good model for what is likely to happen under the Act should section 23 be repealed. The Privacy Act covers the whole gamut of handling personal information from collection to disclosure whereas the OIA only covers requests for information. Additionally, there is usually a presumption of availability under the OIA because disclosure is "necessary" and the public sector is large and can more readily absorb costs of making information available. The Privacy Act on the other hand seeks to guide and inform business decisions which impact on personal information such as formulating policy directions and complaint management procedures within an agency, and the Act provides principles on which good customer relations should be based. Therefore, it is more necessary to require agencies to appoint a privacy officer under the Act to ensure the organisation is complying with the large number of provisions of the Act and to alert management to breaches of the principles and suggest ways to fix these breaches, than it is under the OIA.

An alternative to repealing the entire section is to remove its application to small and medium sized businesses.¹⁸⁶ The problem with this response is the difficulty in finding a universally accepted definition of small to medium sized enterprise, as acknowledged earlier. Assuming one could come to a consensus regarding the size of the organisation to exempt from the requirements of this section, this response should be considered to address the current problem of non-compliance with section 23.

¹⁸⁶ There has been a suggestion that the Act should be amended to only require agencies with 100 or more employees to have a privacy officer: *Compliance Cost Submissions*, above n 12, New Zealand Employers Federation WX3 (24 October 1997). This article does not support this suggestion because the threshold is too high. Instead, this article argues that the threshold should be set at 19 or more employees (based on the definition of "small to medium sized enterprises" being those businesses with 19 or more employees – see Part I Introduction).

Instead of requiring small to medium sized enterprises to have a privacy officer under legislation, the Commissioner could encourage appointment of such a person by educating businesses as to the benefits of this. Even though many of these organisations will only handle very small amounts of personal information (maybe only non-contentious employee records) there is a benefit to them in having an employee knowledgeable in Privacy Act obligations and rights. This person then has the basic skills to assist colleagues, family and friends with any concerns arising under the Act. In other words, educating agencies about the benefits of having a privacy officer helps to build a culture of privacy and growing awareness of the Act. This is discussed in more detail below.¹⁸⁷

It is preferable to maintain the requirement for large enterprises to have a privacy officer. These organisations are more likely to handle large amounts of personal information and, therefore, are more likely to receive information privacy requests and possibly have complaints made against them to the Commissioner. There is a clear benefit in requiring someone to be trained to handle these matters quickly and efficiently. Having this requirement written in legislation sends a clear signal to agencies about the importance of having a privacy officer. However, maintaining this provision for large enterprises requires consideration of how the section is to be enforced.

(b) Penalties for non-compliance

Requiring large enterprises to have a privacy officer necessitates a consideration of penalties for non-compliance with section 23. My experiences in conducting this survey were that about 40 per cent of the companies which apparently did not comply with the requirement to have a privacy officer were large enterprises (those with more than 19 employees). Therefore, non-compliance with this section is not only a concern in regards to small to medium sized enterprises.

Sanctions are needed for non-compliance otherwise the section appears worthless. However, monitoring whether the privacy officer is complying with the section or not is difficult. Non-compliance may only become apparent if the Commissioner has to conduct an investigation because a complaint has been made against the agency. The Commissioner does not have sufficient resources to monitor compliance with this provision on a day-to-day basis. Additionally, it is unlikely that a penalty, such as a fine, imposed for non-compliance with this section would accord with the spirit of the Act. In general, as mentioned earlier, the Act gives businesses flexibility to choose how to meet their privacy obligations. Therefore, imposing a penalty is too heavy-handed for this piece of legislation.

¹⁸⁷ See Part V A Education.

3 Summary

Education by the Commissioner is needed to highlight the benefits of having a privacy officer. Developing a network of privacy officers to discuss issues on an informal level could be useful in increasing the number of designated privacy officers in agencies and the Commissioner's office has now begun this process. If having a privacy officer could become common business practice, at least amongst large enterprises, then formal sanctions would not be necessary because the reputation of the organisation would be tarnished if it were discovered that they had no privacy officer. While it is important to require large organisations to have a person dedicated to ensuring compliance with the Act, this need not be a requirement for small businesses who handle less personal information and therefore have fewer obligations under the Act. Education will increase small to medium sized enterprises' awareness of the importance of fostering a culture of privacy within the organisation. Nevertheless, there are other ways to achieve this besides appointing a person to the role of privacy officer in the case of small to medium sized enterprises. Requiring a privacy officer to be appointed would unnecessarily increase compliance costs for small to medium sized organisations. On balance, section 23 should be amended to only require "large enterprises" (those with greater than 19 employees) to have a dedicated privacy officer. This provision should be strictly enforced by the Commissioner. The requirement should not be kept for small to medium sized enterprises where increased education can help to increase awareness of privacy issues.

D Complaints Provisions

Both ongoing and intangible costs of complying with the Act are increased for an agency where an individual makes a complaint about this agency to the Privacy Commissioner under section 67(1) of the Act.¹⁸⁸ For example, being investigated by the Privacy Commissioner and the subsequent wait for complaints to be dealt with could cause substantial anxiety for an agency. The longer an agency has to wait for the complaint to be resolved, the greater the anxiety.

Literature from the Office of the Privacy Commissioner shows that the Commissioner is trying to address the lengthy delays experienced in complaints investigation and resolution.¹⁸⁹ The complaints backlog level reduced by around 22 percent during the 2003-2004 financial year.¹⁹⁰ At the time of writing the Commissioner had not yet presented the

188 Proposals to reduce the compliance costs associated with the complaints procedure under the Act are discussed in Nicholas Marshall *Protection of Privacy in New Zealand: Is there a Better Way?* (LLM Research Paper, Victoria University of Wellington, 2004).

189 *Annual Report of the Privacy Commissioner for the Year Ended 30 June 2004*, (Office of the Privacy Commissioner, Wellington, 2004).

190 *Annual Report of the Privacy Commissioner for the Year Ended 30 June 2004*, above n 189, 8.

report for the 2004-2005 financial year to Parliament pursuant to section 24 of the Act.¹⁹¹ Therefore, the most recent figures available to show the current trend are those in the 2003-2004 annual report.¹⁹² The biggest inroads, though, were made into reducing the number of longstanding complaints. The proportion of longstanding complaints closed increased markedly from 44 per cent in 2002-2003 to 58 per cent in 2003-2004.¹⁹³ Although these figures suggest the time taken by the Commissioner to investigate and resolve a complaint is reducing, the wait is still quite substantial.

Any moves to further reduce the delays experienced by agencies in having complaints made against them investigated and resolved need to be subjected to a cost-benefit analysis. For example, as part of the 2003 Budget, the government announced further funding for the Office of the Privacy Commissioner to reduce the backlog of complaints¹⁹⁴ and there have been further funding increases since then. Reducing delays reduces compliance costs for those agencies having a complaint made against them under the Act. One respondent to my survey stated that while complaints against their organisation were minimal due to their limited corporate business activities, complaints that required investigation and resolution by the Privacy Commissioner added to compliance costs "due to delays in dealing with the complaints".¹⁹⁵ Therefore, on balance, there appears to be merit in reducing delays to an acceptable level due to the seemingly large costs resulting from such delays.

Additionally, where the Commissioner investigates an agency pursuant to a complaint, ongoing costs to the agency increase enormously. Not only might the agency need to seek legal advice, it also incurs costs relating to employee time to locate any information required by the Commissioner. Possible ways to reduce these ongoing costs include preventing complaints from the outset by the agency being open about its information handling

191 This is due to be presented in October/November 2005.

192 *Annual Report of the Privacy Commissioner for the Year Ended 30 June 2004*, above n 189, 4.

193 *Annual Report of the Privacy Commissioner for the Year Ended 30 June 2004*, above n 189, 21.

194 Hon Lianne Dalziel, Associate Justice Minister "Funding to Clear Privacy Complaints Backlog" (14 May 2003) Media Release. Specifically, funding of \$375,000 was provided in the 2003/2004 financial year and \$222,000 in each of the three following financial years, to allow the Commissioner to "implement a case management approach and improve the processing and resolution of complaints". Additionally, the 2003 Budget also increased funding of the Office of the Privacy Commissioner by \$241,000 in 2003/2004 plus \$207,000 in 2004/2005 to clear the backlog of more than 430 long-standing complaints (as at 31 October 2002) made more than 12 months ago.

195 Citigroup Auckland survey response, above n 104.

practices and adhering to these. However an in-depth discussion of these and other alternatives are outside the scope of this article.¹⁹⁶

E Storage of Information

Another large ongoing cost imposed on organisations by the Act stems from the requirement in Principle 5 that agencies holding personal information do so in a secure manner. This, coupled with the requirements in other legislation making it mandatory for organisations to collect personal information and store it for a certain, sometimes lengthy, period of time, increase costs to an organisation to store information.

This is supported by the findings of my research. Storage of information was one compliance cost that was commonly of concern to organisations. In particular, appropriate storage space, management of secure storage, and disposal of personal information can incur large compliance costs for an organisation.¹⁹⁷ One respondent to my survey suggested that these costs could be minimised by central government through the Office of the Privacy Commissioner subsidising secure storage facilities for documents; or, alternatively, policy makers assessing the need for agencies to retain employment documents (such as wage and holiday records) for such a long period under the relevant employment legislation.¹⁹⁸

On a cost-benefit analysis, such a move would certainly reduce compliance costs under the Act. If directly asked, organisations would be likely to support this proposal. However, given the finite amount of government funds available, this would not appear to be one of the priorities for these funds. And, neither should it be. There are some costs imposed by legislation that organisations should absorb as a necessary part of doing business in New Zealand. This is not a compliance cost that should be shifted from businesses to the government. Instead, the government should analyse the pieces of legislation that require organisations to hold records for certain periods of time. Consideration should be given as to whether the benefits of requiring this information to be kept for a specified period outweigh the costs to an agency of doing so. Further discussion on this matter is outside the scope of this article.

F Summary

This section has discussed specific provisions of the Act that raise compliance cost concerns for organisations in New Zealand. In particular, it has utilised cost-benefit analysis to consider possible amendments to the Act to minimise these compliance costs. However,

196 For further discussion on alternative approaches see Marshall, above n 188.

197 Author's "Privacy Act 1993 Compliance Costs Survey" Fresh Direct Limited response (2 July 2004).

198 Fresh Direct Limited survey response, above n 197.

there are also general overarching ways in which compliance costs could be reduced under the Act. The next section looks at the Act as a whole and suggests general ways in which compliance costs under the Act could be reduced. Specifically, it will be argued that education is the key to minimising compliance costs under the Act.

V GENERAL WAYS TO MINIMISE COMPLIANCE COSTS UNDER THE ACT

A Education

Many concerns about compliance costs can be considerably reduced by education. My survey shows that lack of understanding of the Act and obligations of agencies under it are still key issues for organisations in New Zealand.

One issue for individuals and organisations alike is that the Act is commonly quoted as a reason a business cannot do certain things. Many people have probably received a response from an organisation that "we cannot do that because of the Privacy Act". On some occasions this may be a valid response. However, in my experience the Act is often used as a cover to excuse the agency from doing something that may be against their internal policies, but is not necessarily contrary to the Act. One respondent to my survey supported this experience and argued that "[c]osts could be reduced if people understood the legislation better".¹⁹⁹

This is another way to look at costs imposed by the Act. Such costs are those indirect expenditures incurred by individuals that are caused by failure of the agency to properly understand the Act. These are not "compliance costs" as such and are therefore outside the scope of this paper. However, my experience shows that with adequate education, many "costs" imposed by the Act could be reduced. Educating organisations as to what the Act actually requires and what it does not is the first step to reducing the prevalence of widespread statements such as "we cannot do that because of the Privacy Act". This paper argues that education is the joint role of both the Commissioner and privacy officers in this context. As mentioned earlier,²⁰⁰ the Commissioner has an overarching role to educate organisations about the benefits of having a privacy officer and an obligation to educate the public about the Act itself and individuals' rights under it. Furthermore, the privacy officer has a responsibility to foster a privacy culture within the agency. Indeed, the Act places considerable emphasis on education as being one of the obligations on privacy officers

199 Author's "Privacy Act 1993 Compliance Costs Survey" First New Zealand Capital Holdings Limited response (14 July 2004).

200 See Part IV C Privacy Officer Requirement.

under section 23. Leaving aside the role of privacy officers, as this has been discussed elsewhere in the paper,²⁰¹ this next section considers the Commissioner's role in education.

1 Privacy Commissioner's general functions

Section 13 of the Act lists the functions of the Privacy Commissioner. These functions are quite broad, with an emphasis on consultation with relevant persons and bodies and education of the public and agencies to promote protection of individual privacy. It is encouraging that the Office of the Privacy Commissioner appears to be taking their educative role as provided for in section 13(1)(a) and (g) of the Act seriously. They have made available free of charge plain English guidance notes regarding how agencies can comply with the Act. One respondent to my survey saw this information as being of "considerable value".²⁰² It would help to minimise agencies' compliance costs associated with interpretation of the Act if the Commissioner continued this practice and issued new guidelines as and when necessary.

2 Templates

Such information should be extended to providing templates that comply with the Act for standard documents.²⁰³ There are large ongoing costs to businesses who do not use standardised forms and commercial agreements. One respondent to my survey indicated that excessive compliance costs were incurred in including "conditions [in] all commercial communications with individuals concerning their right to privacy".²⁰⁴

It is likely that this concern would be especially prevalent amongst small to medium sized organisations. Having templates for standard documents may reduce costs incurred in seeking legal advice to ensure that the organisation's documents complied with the Act. These costs could be substantial for small to medium sized organisations. One suggestion is to provide a template document for individuals to complete when requesting access to their personal information and also a template of an employment application form that is compliant with the Act.²⁰⁵ The Commissioner should look at providing templates as these would substantially reduce agencies' compliance costs – especially time – and would require relatively few resources to implement.

201 See Part IV C Privacy Officer Requirement.

202 New Zealand Law Society survey response, above n 87.

203 Fresh Direct Limited survey response, above n 197.

204 Business Professional Services Limited survey response, above n 8.

205 Fresh Direct Limited survey response, above n 197.

3 *Privacy Commissioner's 0800 number*

Standard templates and general information sheets are helpful up to a point to assist organisations in understanding their obligations under the Act. However, their uses are limited to common questions or misunderstandings encountered by organisations under the Act. Where an issue comes up in practice that is not answered by the information sheets and cannot be solved by reference to any of the standard templates, the agency may have to seek costly legal advice. One survey respondent considered that the most significant compliance cost associated with the Act arises from requests that pose novel legal issues and, therefore, require legal advice.²⁰⁶ One way to reduce these legal costs under the Act is to set up an open line of communication between agencies and the Commissioner. Where the agency receives a request that poses novel legal issues, its point of contact should be the Commissioner in the first instance. Where the nature of the question requires legal advice rather than generalised information about the Information Privacy Principles the Commissioner can suggest the agency seek legal advice.

The Commissioner has set up an 0800 number to give organisations an avenue to seek free generalised information on compliance with the Act. Having this "information line" available reduces compliance costs for organisations as it answers straightforward general questions that an agency may otherwise have to go to a lawyer to get answered. The phone lines are staffed during business hours by legally trained people and have a voicemail service for people to leave a message when the lines are busy.²⁰⁷ As long as they can be contacted, people leaving a message receive a response within 24 hours.²⁰⁸

B Greater Use of Codes of Practice

Even education cannot reduce the compliance costs if the Act is not suited to a particular industry. If the provisions of the Act impose unnecessarily harsh restrictions on the ability of an industry to operate in business, then it must be considered whether the application of these provisions to this industry are justified in terms of cost-benefit analysis. In other words, is restricting the ability of an industry to do business necessary in order to protect individuals' privacy interests or could a similar degree of protection still be afforded to individuals without restricting business activities to such an extent? The Act should only inhibit business activities to the minimum extent necessary to protect privacy interests of individuals.

206 New Zealand Law Society survey response, above n 87.

207 Katrine Evans, Assistant Privacy Commissioner (Legal), to the author "Privacy Commissioner's Enquiries Line" (21 September 2004) Oral Conversation.

208 Katrine Evans, Assistant Privacy Commissioner (Legal), to the author "Privacy Commissioner's Enquiries Line" (21 September 2004) Oral Conversation.

Recognising that the application of the Act's principles is not appropriate for all organisations, the Act provides that the Commissioner may from time to time issue a code of practice that modifies the application of one or more of the Principles.²⁰⁹ The code of practice may apply, for example, in relation to one or more specified industries or classes of agencies.²¹⁰ The Act has had a huge impact on credit reporters in New Zealand. The Credit Reporting Privacy Code 2004 seeks to clarify the application of the Act to the credit reporting sector.²¹¹ The inherent tension between the Act and this industry is that in order to do business, credit reporters need to sell personal information to credit providers.²¹² The Act places limits on disclosure of personal information to third parties under Principle 11. Therefore, it is necessary to develop a Code to clarify the application of this and other Principles to the credit reporting industry.

In summary, codes of practice tailoring the Act to certain sectors are a way to minimise compliance costs imposed by the Act. Any codes issued need to stay within the general parameters of the Act, so individual privacy protections need not be compromised. Organisations in industries dealing in personal information, such as the credit reporting sector, are likely to be able to understand their obligations under the Act better if these principles are written in a way that is specific to their industry. Additionally, all organisations would benefit from codes being developed to cover specified personal information, as is intended by section 46(3)(a) of the Act. For instance, the first code set up under the Act was the Health Information Privacy Code 1994. This modifies the provisions of the Act with respect to their application to the health sector. This Code is presented in a very "user friendly" format with each provision of the Code followed by a commentary section on the application of this rule. In the future, the Commissioner could look at developing a code to apply to employee information.²¹³ The vast majority of organisations employ at least one person. Therefore, a code covering this personal information is likely to reduce compliance costs across a wide range of industries. This article supports greater use of codes of practice to minimise compliance costs under the Act.

209 Privacy Act 1993, s 46(1) and (2).

210 Privacy Act 1993, s 46(3).

211 Bruce Slane, Privacy Commissioner "Public Consultation on Proposed Credit Information Privacy Code" (8 July 2003) Press Release.

212 Taylor Duignan Barry Limited *Report on the Costs of Compliance Resulting from the Proposed Credit Information Privacy Code* (Wellington, 2003) paras 5.1-5.2.

213 See Nicola Whittfield's paper supporting the development of a code covering employee's medical information: Nicola Whittfield *Collection and Use of an Employee's Health Information: A Proposed Code of Practice* (LLM Research Paper, Victoria University of Wellington, 2004).

VI CONCLUSION

Compliance costs are a perennial issue that will not go away. Numerous recent compliance costs surveys have ensured that the issue remains in the forefront of legislators' minds. These surveys all come to one conclusion: cumulatively, compliance costs from all legislation are too high and this red tape is stifling economic growth. However, when one looks at the narrow issue of compliance costs and the Privacy Act 1993, the story is somewhat different. While many organisations in New Zealand have the perception that compliance costs under the Act are burdensome, both the Privacy Commissioner's *Review of the Privacy Act: Compliance and Administration Costs* in 1998 and the Ministerial Panel's study in 2001 show that in reality these costs are no more than minor. More recently, my own empirical research has found that this was still the case in 2004. In other words, compliance costs associated with the Privacy Act 1993 are more a theoretical than a practical problem for organisations in New Zealand.

My general impression, formed after conducting research for this article, is that compliance under the Act is largely a matter of good business practice and many businesses would adopt its principles even without legislation requiring them to do so. Where a piece of legislation does not impose any additional obligations on organisations other than those that they would adhere to as part of sound business practices,²¹⁴ compliance costs are minimal.

However, important decisions are often based on perceptions rather than reality and actions are taken on the basis of what people think the legislation says rather than what it actually does say. This article has advocated the need for continuing education to ensure that those working with the Act understand their actual obligations under it and what its practical effects are.

The fact that compliance costs under the Act are not an issue in practice for New Zealand businesses in 2004 does not mean that we can rest on our laurels. Annual surveys such as those jointly carried out by Business NZ and KPMG are an important yardstick against which the success of legislation in minimising compliance costs is measured. However, the results of these general surveys are limited in their application to separate individual enactments such as the Privacy Act because their focus is on the most burdensome legislation. Therefore, there is a clear need to conduct surveys specifically focussed on the Act to truly gauge the ongoing effect of compliance costs in the area of privacy law.

214 Kiwibank Limited survey response, above n 113.

Finally, privacy is not an absolute right. Just as the Commissioner is required to have regard to "the right of government and business to achieve their objectives in an efficient way",²¹⁵ policy makers should also consider commercial interests that compete with privacy when formulating policies. Education of the benefits of complying the Act is the first step to minimise the perception that this enactment imposes a substantial regulatory burden. Indeed, "those companies that master privacy as a competitive opportunity, rather than as a regulatory cost without economic benefit, will be best positioned to remain competitive."²¹⁶

215 Privacy Act 1993, s 14(a).

216 Jeffrey B Ritter, Benjamin S Hayes, and Henry L Judy "Emerging Trends in International Privacy Law" (2001) 15 *Emory Int'l L Rev* 87, 90.

VII APPENDIX ONE

This is the list of questions from the survey that I sent to 50 New Zealand organisations in June 2004.

- (1) What are compliance costs?
- (2) Are there any aspects of the Privacy Act that cause excessive compliance costs?
- (3) What more could be done to reduce compliance costs? What else could be done to minimise compliance costs, in particular for smaller businesses?
- (4) What actual business costs are involved in complying with the Privacy Act?
- (5) Could the layout or wording of the Privacy Act be improved to make it easier to use?
- (6) Should more cost recovery for access and correction requests be allowed to reduce agencies' compliance costs?
- (7) How do delays in dealing with complaints affect compliance costs? What measures could reduce the time for complaints investigation and resolution to reduce compliance costs?
- (8) Can the Privacy Officer's role be enhanced in some way relevant to effective use of resources in regard to compliance?
- (9) What specific compliance costs incurred are of most concern? In what ways could these be reduced?
- (10) 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 helpful in reducing compliance or other costs?
- (11) Are there other mechanisms that could usefully cater for the specific needs and practices of agencies or sectors to reduce compliance costs? Should New Zealand leave the regulation of privacy in the private sector to industries to develop their own codes of practice?
- (12) If you made submissions in 1997 in response to the discussion paper entitled "Compliance and Administration Costs" issued by the Privacy Commissioner, how has your thinking differed in relation to the issue of compliance costs in the last seven years? Have they increased, decreased or stayed relatively the same during this period? What is the basis for your answer?

VIII APPENDIX TWO

Organisations that responded to my questionnaire were:

- Citigroup, Auckland (19 July 2004)
- First New Zealand Capital Holdings Limited (14 July 2004)
- Fresh Direct Limited (2 July 2004)
- Victoria University of Wellington (15 July 2004)
- Business New Zealand (1 July 2004)
- Ministry of Education (24 June 2004)
- Business Professional Services Limited (14 July 2004)
- New Zealand Law Society (21 June 2004)
- Franklin District Council (undated, returned July 2004)
- Kiwibank Limited (via telephone, 14 July 2004)

