Privacy Commissioner
Te Mana Matapono Matatapu

Report of the Privacy Commissioner

for the year ended 30 June 1998

Presented to the House of Representatives
pursuant to Section 24 of the Privacy Act 1993

December 1998

Rt Hon Doug Graham MP
Minister of Justice
WELLINGTON

I tender my report as Privacy Commissioner for the year ended 30 June 1998.

B H Slane
Privacy Commissioner

CONTENTS

Figures and Tables

I. Introduction

Failure of agencies to explain themselves

In the submissions made to me during my review of the operation of the Privacy Act, the only common criticism of the operation of the Act was that it was being wrongly cited to fob off people with legitimate requests. Essentially the criticism was that the agencies concerned either wrongly cited the Privacy Act or were oblivious to its application and took no responsibility for their own policies. In many cases they were either unaware of what their staff were telling people or cared little about the bad public relations this created. My message has been clear: in most cases agencies can set their own policies, so "blaming" the Act is not appropriate.

Many businesses and Government agencies make a point of emphasising their commitment to service for their clients, customers or those who have to use their services. Telling such people that the Privacy Act prevents them from doing something when that is not the case undermines any commitment to openness or fair information practices.

During the year my staff and I followed up a number of cases where our attention was drawn to this sort of behaviour. In some cases we found that managers were unaware that the expression "because of the Privacy Act" was being tendered as an explanation in situations where it was not applicable or where a more informative explanation was warranted.

The most common of these was where the request ought to have been dealt with under our freedom of information laws, the Official Information Act or the Local Government Official Information and Meetings Act. This highlights the failure of training about the Official Information Act in public sector agencies.

One recommendation which came out of a recent Law Commission report was for the Ministry of Justice to take a more active education role in relation to the Official Information Act.

A significant role of my workshops is to explain the relationship which is comparatively straightforward. Very often we have found attendees to have a good understanding of the Privacy Act but to have never been trained adequately in dealing with Official Information Act requests. As a result of training and advice on the office hotline to individuals, the prevalence of this excuse has tended to drop off during the year.

Privacy and Freedom of Information

These situations have been put forward to support a suggestion that

there ought to be a Freedom of Information Commissioner. This is a role which is used in some Canadian jurisdictions to promote systemic dissemination of publicly held information as well as deal with individual complaints. In some provincial jurisdictions where privacy and freedom of information laws apply only to the provincial government apparatus, the same Commissioner deals with both privacy and information.

However, privacy and freedom of information are not obverse sides of the same coin, as the Canadian Federal Privacy Commissioner has pointed out. Privacy is a fundamental human right. Freedom of information contributes and is very important to democratic government. (There is some commonality in that many FOI laws give a right to individuals to access their own information, as did our Official Information Act until that right passed into the Privacy Act in 1993.) In practical terms, the promotion of accountability of the Government and the participation of people in a democratic process should not generally require the dissemination of personal information about identifiable citizens. When personal information is involved in third party access requests, privacy considerations have to be taken into account.

Some newspapers have promoted the idea that my role is to be a zealot who pursues privacy issues to the detriment of freedom of information. This of course is a nonsense, as would be seen from reading section 14 of the Privacy Act which requires me to have regard to social interests which compete with privacy, including the desirability of a free flow of information and the need for government and business to carry out their functions efficiently.

In all of the reports on new legislation and the consultations undertaken with Government officials on new proposals my staff and I have to balance these competing interests. We cannot and do not put privacy forward as the only issue to be considered.

Similarly, an information commissioner would have to have regard to privacy values.

People who are fobbed off are encouraged by my office to question whether or not it is the agency's own policies or the Act which requires the agency to take the position it espouses. They are encouraged to seek precise reasons for an agency's actions. They are also advised to contact the privacy officer of the agency if in any doubt. Of course, in many cases, there are good public interest reasons for there to be Privacy Act consequences for unanticipated disclosures of information. But to suggest that information is not being disclosed because of the Privacy Act rather implies to the listener that, but for the Privacy Act, the information would be readily made available. In many cases, investigation has revealed that the agency has never disclosed such information either routinely or

in response to specific requests.

Information can always be used for the purposes for which it was obtained and if that involves disclosure, it will be in accordance with principle 11 or some other enactment. This reliance on purpose does entail responsibility to ensure that open information practices are applied to personal information, and this seems to be a problem for some agencies, which look on privacy concerns as a risk to be managed, rather than as an integral part of information management.

Health information: a real public concern

The issue also crops up in the health sector, where training has been a real issue. I am planning to undertake more training initiatives in that area.

Open information practices are particularly important in the health sector. A survey I commissioned during the year revealed that very large sums of money have been expended on planning and developing schemes for gathering people's health records into new information flows to meet perceived efficiency needs. In most cases, little or no consultation has taken place with my office and I have been unable to put resources into exploring the technological and privacy issues involved in these plans.

There are significant risks for the Government, which is the major funder of such proposals, because in the end these schemes will depend on public acceptance and confidence. I do not believe that that confidence can truly be assured at present. It seems remarkable that funds are so readily available in the health sector to progress unpublished plans without taking the public into confidence or providing adequately for those whose sensibilities about their personal information cause them to distrust further gathering of that information away from the providers with whom they choose to deal.

Much money expended on these proposals could be wasted if they proceed without the design incorporating proper privacy protections. They may exceed statutory powers or so offend privacy principles that codes of practice may become necessary. That was why last year I sought funding especially devoted to this area. Because of economic constraints the Government declined to make any further provision.

The task of a Privacy Commissioner in these circumstances is to bring such proposals out into the daylight and to examine them for considerations besides the business efficiency which has driven them. It is simply not good enough at this stage of our development to have proposals to gather sensitive information for unspecified purposes because it might be useful to have these records in the future.

Resourcing

The review of the operation of the Act which I chose to carry out in an open and comprehensive way was a large undertaking for a small office. This activity, which is to be carried out at five yearly intervals, is not specifically funded. Therefore during the year I had to defer work on some other areas which are now becoming very urgent. I am obliged under the Act to review the case for continuing existing provisions for information matching and the first of these reports will be completed in the coming year.

Work has been deferred in relation to codes of practice which have been proposed for telecommunications and credit reporting. Both of these are large undertakings and will involve the weighing of some competing interests.

I am heartened by the degree of public support this office has been receiving. There is an enormous amount of goodwill for the work that my staff are carrying out and much greater realisation of the importance to an agency of the integrity of its information and of its information handling policies and practices.

Privacy issues would exist whether or not there was a Privacy Act. They would have to be dealt with and there would be costs involved in doing so. I believe the compliance costs borne by industry and Government under the Privacy Act are probably very little more than they would have in dealing with the uncharted territory of fair information practices. This is made so much easier by the existence of the information privacy principles. It is clear from developments in Australia involving voluntary self regulation that such schemes, if they are to be effective, do not produce compliance costs lower than a statutory regime.

II. Office and functions of the Privacy Commissioner

The Privacy Commissioner is independent of the Executive. This means that I am, and can be seen to be, free from influence by the Executive when investigating complaints. This is important because I am from time to time called on to investigate complaints against Ministers or their departments and ministries. My independence is also important for some of my other roles, such as examining the privacy implications of proposed new laws and information matching programmes.

I have a responsibility to report to Parliament through the Minister of Justice, and am accountable for my functions as a crown entity under the

Public Finance Act.

When exercising my functions, the Privacy Act requires me to have regard to the information privacy principles and to the protection of the human rights and social interests that compete with privacy. This includes 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. I must also take account of international obligations accepted by New Zealand, including those concerning the international technology of communications, and consider any developing general international guidelines which are relevant to the better protection of individual privacy.

One of my functions is to receive and investigate complaints and provide an independent opinion as to whether there has been an interference with privacy. I do not act as an advocate for either party: my role is impartial and investigative. My role also includes acting as a conciliator to try to resolve complaints. Complaints made to my office may be referred to the Proceedings Commissioner (appointed under the Human Rights Act), who may bring civil proceedings before the Complaints Review Tribunal. I refer very few complaints to the Proceedings Commissioner, as most of them are resolved satisfactorily during my investigation process.

I also have a function of promoting by education and publicity an understanding and acceptance of the information privacy principles. I have had an enquiries team available to answer questions and have for several years maintained a toll free hotline so that people may make enquiries without charge from anywhere in New Zealand. This service has had to be restricted.

As part of my educative role, I have maintained a website from which people may download information about the Privacy Act at no charge. My website contains many publications, including codes of practice, casenotes, fact sheets, speeches and reports. During the final half of the year, my website was being rebuilt and the new website was expected to be online early in the next year.

I also conduct workshops and seminars and maintain open communication with the news media.

Another of my responsibilities is to monitor government information matching programmes which must be carried out in accordance with the provisions of the Privacy Act.

I have a function of issuing codes of practice which can modify the information privacy principles by:

- prescribing more stringent or less stringent standards than are prescribed by the principles;

- exempting any action from a principle, either unconditionally or subject to any prescribed conditions.

A code may also prescribe how the information privacy principles are to be applied or complied with.

One of my functions is to make public statements on matters affecting privacy. Speaking publicly on issues I may act as a privacy advocate, but must have regard to wider considerations. One of my most significant roles is to comment on legislative, policy or administrative proposals which have some impact on the privacy of the individual or classes of individuals. Many of my recommendations are adopted by government departments, cabinet committees or by select committees in the course of their consideration of policy and legislative proposals. In every case I have had to balance privacy interests against the interests which compete with privacy.

Other functions of the Privacy Commissioner are found in section 13 of the Act. They include:

- monitoring compliance with the public register privacy principles;
- making suggestions to any person in relation to the need for, or the desirability of, action by that person in the interests of the privacy of the individual;
- reporting to the Prime Minister on any matter that should be drawn to her attention and, particularly, the need for and the desirability of taking legislative, administrative or other action to give protection or better protection to the privacy of the individual.

REVIEW OF THE OPERATION OF THE ACT

Section 26(1) requires the Privacy Commissioner to review the operation of the Act as soon as practicable after the Act has been in force for three years, and thereafter at intervals of not more than five years. The review must conclude with a report to the Minister of Justice on the findings and make recommendations about any necessary or desirable amendments to the Act. The first such review has been a major undertaking during the year.

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

agencies participating in authorised information matching programmes.

Section 26 does not require the review to be conducted in any particular way. However, I decided very early on to consult fully. Given the nature of the Privacy Act, this meant consultation not only with Government and business but with the public as well. I advised the Minister of Justice of my intention to undertake public consultation and a statement to this effect was made by the Minister in Parliament in August 1996. The public phase of the review started about the time of the Act's fourth anniversary, with the report expected to be finalised and submitted to the Minister of Justice shortly after the fifth.

Many people with useful experience with the Act might have been discouraged by a single large consultation document, so my office released 12 discussion papers over a period of several months, allowing people to choose to contribute according to their experience or interest. As Table 1 shows, the first eight papers corresponded to relevant Parts of the Act while the balance considered the themes of compliance and administration costs, interaction with other laws, intelligence organisations and the Act, and new privacy protections. The discussion papers drew primarily on ideas and issues generated or identified within my office, or in responses from departments and representative bodies to my earlier letters and the information matching questionnaire.

TABLE 1: DISCUSSION PAPERS AND NUMBERS OF SUBMISSIONS

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

I was pleased with the response. While submissions were received beyond the closing date of 10 November 1997, most were to hand by February 1998. The submissions were acknowledged, numbered and compiled into four volumes, which were provided to the Ministry of Justice in February 1998 and have been available for public inspection or purchase from my office since then.

I held a series of public consultation meetings in November in the four main centres, allowing people who had made written submissions to elaborate upon issues of concern. I then held a further series of meetings between myself, my staff, and invited experts during December. A consultation meeting was also held with local government.

During the first half of 1998 I continued to study the submissions and research the issues raised. In some cases, further details were solicited from people who had made submissions. In others, specialist drafting or technical advice was sought. As material was prepared, I further consulted with people who had relevant expertise and with some agencies which might be specifically affected by recommendations under consideration. Much of the report had been written by the end of the year and I expected to submit it to the Minister of Justice in the first half of 1998/99.

STAFF

Staff are employed by the Privacy Commissioner in the Auckland and Wellington offices. I have had the benefit of an acting general manager on a short term contract who has had responsibility in relation to both offices. The manager for investigations is based in the Auckland office and is assisted by a complaints team leader in each office. The Manager, Codes and Legislation reports directly to the Commissioner and has an officer reporting to him.

The enquiries officers, executive officer and accounts clerk report directly to the Privacy Commissioner.

As in previous years, the volume and nature of the work required a great deal of all who were employed. Although the number of incoming complaints has dropped, the length of the queue has put considerable pressure on the Manager Investigations and the investigating officers. They have maintained high standards in their work and have maintained a rapport with the agencies they commonly come into contact with.

The enquiries team has dealt with a significant increase in enquiries with patience and dedication.

The office has again been well served by its support staff, without whom the work of managers and staff would be considerably more difficult.

At 30 June 1998 the following staff were located in offices in Auckland and Wellington.

Marilyn Andrew	Support staff (part-time)
Wendy Bertram	Codes and legislation officer
Joanne Cairns	Investigating officer
Heather Day	Investigating officer
Terence Debenham	Senior enquiries officer
Michelle Donovan	Investigating officer (part-time)
Frances Ermerins	Support staff
Margaret Gibbons	Support staff
Sandra Kelman	Investigating officer
Sarah Kerkin	Executive officer
Kristin Langdon	Complaints team leader
Eve Larsen	Support staff (part-time)
Ian MacDonald	Enquiries officer
Tania Makani	Enquiries officer
Deborah Marshall	Manager, Investigations
Sharon Newton	Support staff
Glenda Osborne	Accounts clerk (part-time)
David Parry	Investigating officer
Gillian Rook	Support staff
Amir Shrestha	Support staff
Silke Simon	Complaints team leader
Blair Stewart	Manager, Codes and Legislation
Joanne Torrens	Support staff (part-time)
Marjorie Warwick	Librarian (part-time)
Michael Wilson	Investigating officer

I have also been well served by Gary Bulog, Susan Pilgrim, Robert Stevens, Graham Wear and Janice Lowe who have been engaged in legal, advising, investigative or publication work for me.

III. Report on activities

GENERAL

The lack of resources to process complaints and reviews have led to real injustices and second-class treatment of people with privacy complaints compared with those who make complaints under the Official Information Act, the Ombudsmen Act, the Human Rights Act or the Health and Disability Commissioner Act. There is no doubt that some people do not pursue a complaint because of the delay of about a year which would be entailed in many cases before it could be allocated to an investigating officer. In these circumstances I believe that the 9% drop in new complaints should not be regarded as a good result for underfunding. The dissatisfaction that those complainants have with the agency continues, and the agency may or may not be aware of it.

Often the agencies would prefer to have the matter resolved in a reasonable time under the non-adversarial approach taken by my office with an emphasis on conciliation, rather than to leave the sore to fester. In some cases only a small amount of time would need to be spent to bring about a resolution. Many businesses have expressed disappointment that we cannot resolve complaints because they are ready to have them dealt with and my office is not.

Since the beginning of this office, the emphasis has been on encouraging compliance by agencies rather than promoting complaints from members of the public. I do not believe that encouragement of complaints would produce better outcomes. But complaints do highlight deficiencies in systems. Some good compliance work is carried out by my investigating officers when dealing with such complaints. Therefore some of the expenditure on complaints investigation could really be regarded as an education function.

One of the reasons I believe it is not necessary to educate every member of the public about privacy rights is that most people, in the experience of this office, have a pretty good idea when something has gone wrong with their personal information that there has been a breach of their privacy. We do not have a large number of approaches made to the office where there is no question of having any jurisdiction or where the complaint is trivial or vexatious.

I must record again my gratitude to members of my staff for the way in which they have engaged in the activities of the office. In complaints investigation a great deal of diplomacy and firmness is necessary, but I believe in the vast majority of cases both parties come to accept the impartial position of the office even if one or other of them might feel that the conclusion

reached is not correct. Although sometimes government departments with new policy proposals may consider the Privacy Act simply as a problem to be overridden by another law, my Manager, Codes and Legislation or his legislation officer have been able to persuade them that there are better ways of going about their objectives or to suggest a compromise that would achieve their objective while minimising the invasion of privacy. Departments have expressed their appreciation of the approach taken.

CODES OF PRACTICE

Under Part VI of the Privacy Act I may issue codes of practice in relation to agencies, information, activities, industries, professions or callings. During the year I issued one new code of practice and began consultation on amendments to another. I did not issue any codes of practice in relation to public registers under Part VII of the Act.

Health Information Privacy Code 1994

The Health Information Privacy Code 1994 remains in effect and, in my view, has continued to provide a satisfactory set of rules for maintaining privacy in relation to the sensitive personal information obtained, held and used in the health sector. In 1998 I released two proposed amendments to the Code, primarily to address technical issues. These amendments had not been issued at the end of the year.

Superannuation Schemes Unique Identifier Code 1995

This Code, which was outlined in an earlier report, remains in force. I did not receive any complaints in relation to the Code and did not make any amendments.

EDS Information Privacy Code 1997

This Code, outlined in last year's report, came into force on 1 July 1997 and will remain in force until 30 June 2000. I did not receive any complaints and did not make any amendments.

The Code establishes procedures to be followed if specified personal information is to be transferred off-shore for processing and requires notice be given to the Privacy Commissioner of any proposed transfer. Some communications were received during the year about the transfer of data from one designated agency to the USA for analysis following processing problems. The matter remained under consideration at the end of the year.

Justice Sector Unique Identifier Code 1998

In February 1998 I released the Justice Sector Unique Identifier Code for public consultation. It was issued on 3 April and came into force on 30 June.

Since the mid-1970s all justice sector agencies have relied on a single integrated computer system for storing and processing law enforcement information. This system, formerly known as the "Wanganui Computer System", allowed justice sector agencies to record and access details about individuals being processed through the criminal justice system by means of a common identifier known as the personal record number (PRN). The PRN ensured that key data, such as criminal history, were ascribed to the correct individual.

From June 1998, all justice sector agencies will be moving from the present integrated computer system to their own independent information systems. The process is expected to be complete by December 1999.

Accurate identification of individuals moving through the criminal justice system is of significant importance to the maintenance of the law, the operational needs of law enforcement agencies, and for the individuals concerned. The use of a single identifier within the criminal justice system was therefore desired and would, in some respects, continue the practice followed under the Wanganui Computer Centre Act 1976 with the PRN. However, assignment of a shared identifier was precluded by information privacy principle 12. The Code addressed agencies' compliance difficulties by permitting a single unique identifier to be assigned by all agencies within the criminal justice sector.

The controlled use of a shared identifier could contribute to the protection of privacy in two respects. First, it would guard against the possibility of incorrect information being associated with the wrong individual (for example, a conviction being recorded against the wrong John Smith). Second, it would remove the need for an individual's name and address to accompany records being transferred on-line between justice sector agencies.

The unique identifier was originally to be called the "Justice Offender Reference Number". As a result of consultation, it was retitled "Law Enforcement Agency Reference Number" (LEARN) to avoid the association of accused persons with an identifier using the word "offender" before they had been convicted. The LEARN may not be used for other purposes such as identification of victims, witnesses, licensed drivers or firearm owners.

Regulations Review Committee

Codes of practice issued under the Privacy Act are deemed to be regulations for the purpose of the Regulations (Disallowance) Act 1989.

This provides safeguards in case a Commissioner makes an unexpected or unreasonable use of the code of practice power.

The first safeguard involves the disallowance procedure provided by the 1989 Act itself, which enables members of Parliament to seek to have Parliament disallow or amend a code of practice. That procedure has not been used in respect of any code of practice issued under the Privacy Act.

A second set of safeguards arises because, as deemed "regulation", codes of practice are subject to scrutiny by the Regulations Review Committee of Parliament. That Committee can examine a regulation on a complaint by a member of the public or agency or on its own initiative. The Committee has not received any complaints about a Privacy Act code. However, all regulations are referred on a routine basis to the Committee, which peruses them and may, on occasion, ask for some explanation of a provision or commence a more thorough inquiry. In this way, the Committee has considered several codes.

In 1995, the Committee made some informal inquiries of the Office of the Privacy Commissioner concerning the issue of the GCS Information Privacy Code 1995. The Committee wished to know whether I had been asked to issue that code of practice or whether it was of my own initiative. This year, the Regulations Review Committee inquired of the Privacy Commissioner as to the purpose of the Justice Sector Unique Identifier Code. I offered a detailed response which satisfied the Committee. The Chairperson of the Committee took the opportunity to commend my office on the plain language drafting of the code.

COMPLAINTS

Complaints received

Figure 1 shows the outcome of the complaints on hand at the beginning of the year (790) and those received during the year (1082). Of these, 804 were closed during the year and 1068 were current at 30 June 1998.

The number of complaints I received during the year showed a decrease from last year of just over 9%, which was not entirely unexpected. As agencies become more familiar with the Act and have policies and staff training in place to ensure compliance, the number of incoming complaints should level off. It is also possible that the decrease has been influenced by the implementation of the queuing system. I have made no secret of the fact that I am insufficiently resourced to investigate the complaints I have on hand. I should not be surprised if

FIGURE 1: COMPLAINTS RECEIVED AND CLOSED 1995 -98

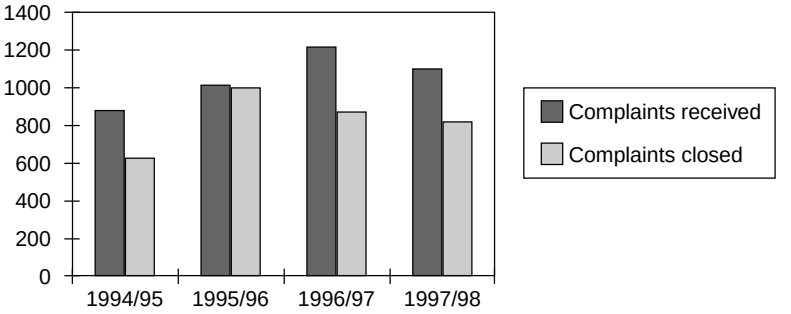
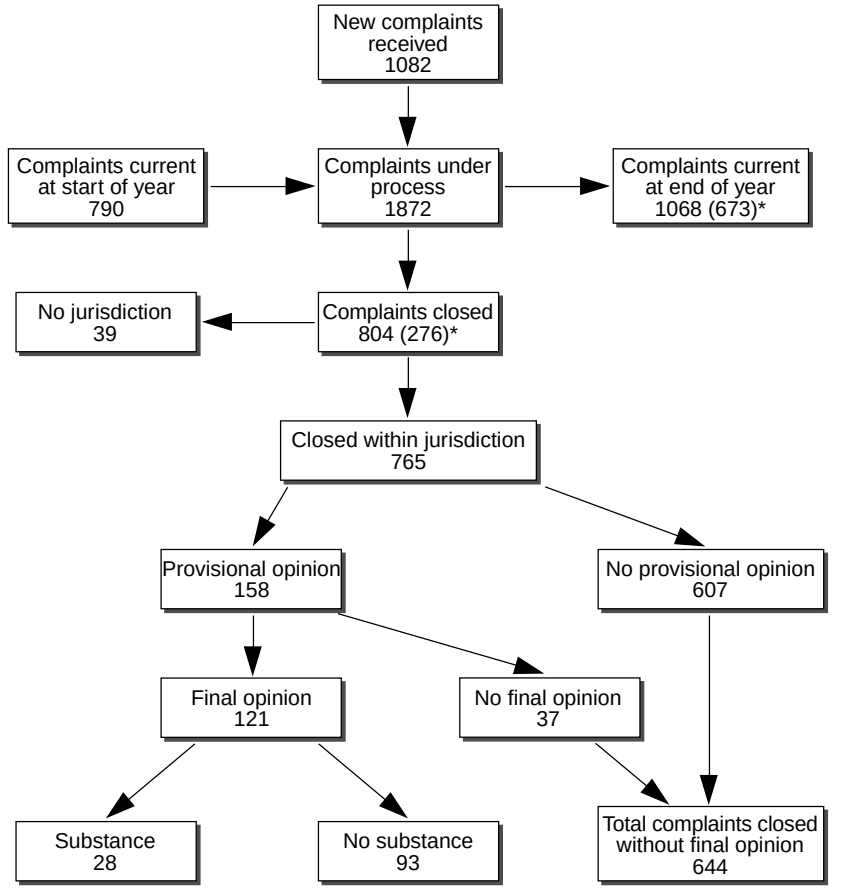


FIGURE 2: ANALYSIS OF COMPLAINTS PROCESSED IN THE YEAR ENDED 30 JUNE 1998



* Queued complaints

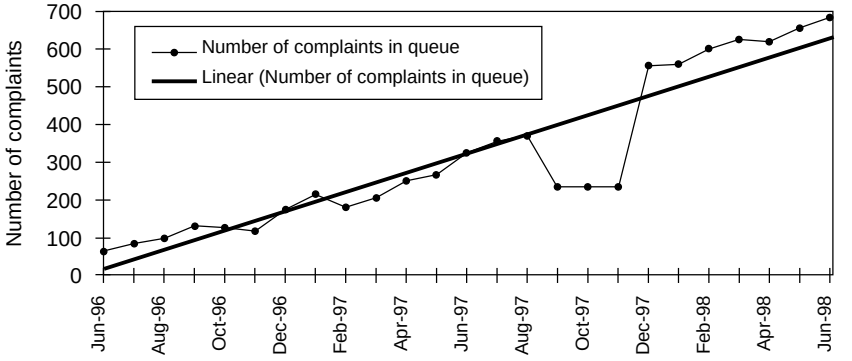
the prospect of waiting nearly a year for an investigation has dissuaded some people from making a complaint.

It should not be concluded from the analysis (figure 2) that only 28 of the complaints had substance. The Act requires me to try to settle complaints between the parties wherever possible and to seek an assurance against repetition of the action that is the subject-matter of the complaint. A large proportion of the complaints which did not proceed to a final opinion had merit which was recognised by the agency concerned and significant settlements were reached in many cases.

Queued complaints

Complaints have been received at a greater rate than I could investigate with the resources provided to me. To assign new complaints immediately to investigating officers would quickly result in an unmanageable workload for those officers who each handle on average 40 to 50 current complaints at a time. While some complaints had to be dealt with urgently, most were placed in a queue to be allocated as existing complaints were closed. At the year end, complainants could wait about eleven months from making the complaint until an investigating officer was assigned to their case.

FIGURE 3: NUMBER OF COMPLAINTS IN QUEUE BY MONTH TO JUNE 1998



The queue continues to grow and in an effort to control this I have sought to resolve as many complaints as possible at an early stage. This does not occur without effort on the part of my staff.

I review each complaint as it comes in and my staff may attempt to resolve the matter informally by telephoning either or both parties and suggesting a way of settling the matter. In some cases it is possible to

write to the complainant outlining the relevant provisions of the Act and suggesting, based on previous cases investigated by me, the possible outcome of the investigation. Some complainants choose not to continue with their complaint at this stage. In other cases it is possible, once further information is received from the complainant or respondent, to settle the matter before it is assigned to an investigating officer.

If the complaint cannot be quickly and informally resolved, I write to both parties acknowledging the complaint and advising them of the queue system. The respondent is given brief details of the complaint and invited to try to resolve the matter in the interim. My staff will assist in effecting any resolution. Some agencies are energetic in their attempts to sort the matter out, realising that a quick resolution will, in the end, save them the time and resources involved in being a party to an investigation. A speedy response is also seen by some complainants as a positive indication of that agency's commitment to privacy issues.

Examples of early resolution of complaints:

- A complainant made an appointment to see a bank officer at her bank to discuss her redundancy and the financial problems flowing from it. She alleged that the interview took place within the hearing of other customers waiting for service. Having been notified of the complaint, the bank contacted the complainant and apologised. The bank advised that renovations would separate the waiting area from the personal bankers by a partition. The bank also proposed to give staff additional Privacy Act training and would remind staff to ask customers whether they wanted interviews to be conducted in a private meeting room. The complainant was satisfied with the bank's actions.
- A complainant's prescription was part-filled by a pharmacist, but he did not have sufficient stock to complete the prescription. It was arranged that the complainant would return on another day to pick up the rest of the medication. That evening the pharmacist's assistant delivered the medication to the complainant's home, explaining that she lived nearby and the pharmacist had been concerned that, as the complainant lived in a rural area, it might be inconvenient for her to return to the pharmacy. The complainant considered that the pharmacist's use of information on the prescription form relating to her home address amounted to an interference with her privacy. My staff wrote to the complainant, explaining that for there to be an interference with privacy a privacy principle would have to be breached and some harm to the complainant would have to arise from the breach. Although the complainant had been annoyed at the visit, it was not considered that this was sufficient harm and I discontinued the investigation.

Investigation of complaints

Complaints which are not resolved are eventually assigned to an investigating officer. Both parties are advised of the investigating officer's name and are given information about the investigation procedure. They are encouraged to contact the investigating officer to discuss possible settlement options.

Many of the complaints investigated can be settled without the need for me to form an opinion on the substance of the complaint. Section 74 of the Privacy Act provides that I may attempt to secure a settlement between the parties, where it appears possible, and I have incorporated this into my investigation procedure. Where appropriate, I may also attempt to obtain a formal assurance against the repetition of the action which is the subject matter of the complaint.

Settlement can be achieved in a number of ways. In some cases an explanation of some action is given or an apology is offered and, if the complainant is satisfied, I may close the file. Other cases may involve the payment of some compensation or some other restorative action undertaken. Complaints involving access to information are often resolved once the individual receives the information requested. (In other cases the delay may have caused the requester a loss.)

In some cases, I may establish that the facts given by the complainant are inaccurate and conclude that further investigation of the complaint is unnecessary or unwarranted in the circumstances. In such cases I would discontinue my investigation without forming a provisional opinion. Similarly, where an explanation seems on investigation to be credible, I advise the complainant accordingly. The complainant may be satisfied with the explanation, which may be accompanied by an acknowledgment of the reasonableness of the complainant's attitude, and not want the matter to proceed further. I am continually impressed by how many complainants will accept a modest settlement despite the outrage they feel at the action of the agency. It should not be thought that these cases are minor or of no importance. I believe the settlements reflect reasonableness on the part of many complainants, particularly when met with a conciliatory stance from agencies and is a credit to the non-adversarial nature of the process.

If settlement is not achieved I give my provisional opinion on the complaint. That may resolve the complaint but, if not, I may give a final opinion on whether the complaint has substance. I will usually try to obtain a settlement at that stage.

Of the 765 complaints which were closed within my jurisdiction, 644 were closed without my having to form a final opinion on the substance of the complaint.

The following examples indicate the sort of settlements routinely achieved:

- A complainant resigned from his employment. His former employer then sent a letter to affiliated organisations advising them of the cessation of the complainant's employment and detailing perceived inadequacies of his work performance. The former employer agreed to a monetary settlement of the complaint without conceding whether or not the disclosure had been made in breach of the Privacy Act.
- Two complainants alleged that serious allegations held on their daughter's file by the Department of Social Welfare were inaccurate. They wanted the Department to destroy the information. The Department was not prepared to destroy the letter in question as it considered the information might be needed in the future. However the Department offered to place the letter in a sealed envelope with instruction that it not be opened without the authority of a specified senior member of staff. In this way the letter would not be read routinely in conjunction with the daughter's file. The complainants were satisfied with this arrangement.
- A bank inadvertently sent information about a complainant to another of the bank's customers. The complainant had reasons for wanting to keep his financial information confidential and was distressed by the disclosure. The bank apologised to the complainant and paid $3,000 in settlement of his complaint.

In 158 complaints I gave a provisional opinion. In 37 instances my staff were able to resolve the matter before I needed to arrive at a final opinion.

Of the 121 complaints in which I proceeded to a final opinion, I concluded in 28 cases that the complaint had substance in whole or in part. In many of these cases, following the final opinion, it was not necessary to take any further action. With some, further efforts were made to secure a settlement.

Access complaints

The right of access to personal information is an important right. It increases accountability in public and private sector agencies. Use of the right of correction helps to ensure that decisions affecting people are made on the basis of accurate and up to date information.

Access complaints are essentially calls for review of a decision not to make available some or all personal information to a requester. Many are resolved after further information has been made available. Thirty-two per cent of complaints received this year involved an access review. Forty-nine per cent of those complaints were made against private sector agencies.

FIGURE 4: COMPLAINTS INVOLVING ACCESS AS A PERCENTAGE OF TOTAL COMPLAINTS 1995-98

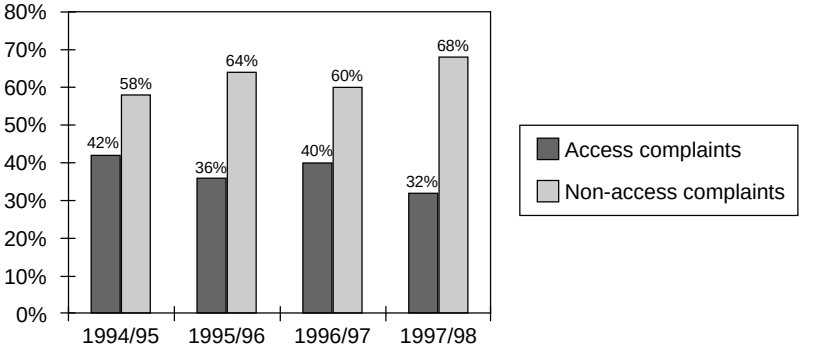


TABLE 2: ACCESS COMPLAINTS BY SECTOR 1995-98

	1994/95	1995/96	1996/97	1997/98
Private Sector	150	176	256	170
Public Sector	218	181	206	179
Total	368	357	462	349

Five years have passed since the Privacy Act came into force and it is of concern to me that some agencies still do not appear to be aware of people's right of access to personal information. However, complaints involving access are at a slightly lower level than in any previous year and the lowest as a proportion of total complaints. Many complaints are made to me alleging that a request for information has been made to an agency and either no response has been received or the request has been refused inappropriately. Many of these requests are in the health sector, which could improve its record in this area. For example:

- A complainant asked a doctor for information held about her and did not receive a response to her request. The doctor was contacted by my office. He had not responded to the request because he had been concerned that access to the complainant's notes might affect her psychiatric condition. He then sought advice from other health professionals and subsequently made the entire file available to her.
- The complainant requested access to notes held about her by her GP. Her request was refused but no explanation was given. The GP was contacted and it appeared that she was not aware of the provisions of the Health Information Privacy Code which gave the complainant a

right to access, subject to certain withholding grounds. A copy of the relevant provision was sent by facsimile to the GP, who then made the information available to the complainant.

TABLE 3: ACCESS COMPLAINTS BY OUTCOME 1997/98

Outcome	Number
Opinion – substance	18
Opinion – no substance	46
Settlement	71
Investigation discontinued	214
	349

Where I consider an agency has a proper basis for the decision to withhold information requested I form the opinion that the complaint has "no substance". Thirteen per cent of access complaints had no substance. In 61% of access complaints the investigation was discontinued. Many of these cases involved a dispute between the agency and requester about what information existed or had been made available. In such cases the agency might provide an explanation to me, which is passed to the complainant. Often I receive no further correspondence from the complainant and the investigation is discontinued.

Alternatively, the agency might provide me with reasons for withholding the information. I am then able to write to the complainant outlining the likely outcome of further investigation, based on previous cases I have investigated. Again, many complainants do not require any further action from my office at that stage.

In other cases, I might consider that in all the circumstances it would be inappropriate to continue the investigation, perhaps where the respondent has made significant efforts to resolve the matter but the complainant remains dissatisfied. This might occur where the Privacy Act issue is but one small part of the dispute between the parties.

It must be borne in mind that requesters have no way of telling whether they have received all the information about themselves or, in many cases, of telling whether a withholding ground has been correctly applied. It is only the intervention of my office which views the files and considers withholding grounds that can establish whether or not the review was justified.

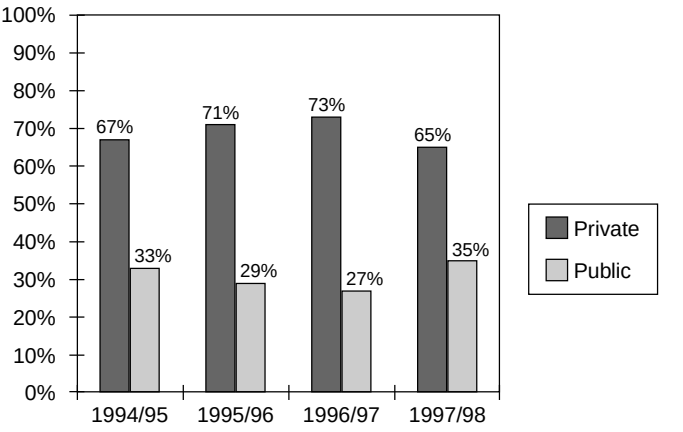
In many cases listed as discontinued my intervention has resulted in

further information being made available. In such cases I do not usually find it necessary to make a final finding of substance.

The procedure in my office, based on that of the Ombudsmen, is the only effective way of dealing with access. Under the Privacy Act complainants who are dissatisfied with the outcome can refer the complaint to the Complaints Review Tribunal and can claim damages for any loss or harm they have suffered. This is a considerable advantage over the Official Information Act.

Disclosure of information

FIGURE 5: COMPLAINTS ABOUT DISCLOSURE OF INFORMATION 1995-98



These complaints involve allegations of disclosure contrary to information privacy principle 11. Disclosure complaints continue to form a significant proportion of the complaints received by me. Complaints against the private sector are the lowest so far. The public sector complaints have been consistent at about 100 over the last four years.

TABLE 4: DISCLOSURE COMPLAINTS BY SECTOR 1995-98

	1994/95	1995/96	1996/97	1997/98
Private Sector	206	250	271	195
Public Sector	103	102	100	105
Total	309	352	371	300

Some typical complaints about disclosure are as follows:

- A Council video-recorded the complainant watering her garden on a day when people in her area were banned from doing so. She understood that the film was to be used for Council purposes. She later found out that the film had been used in a national television news broadcast and complained that the Council had disclosed the film to the television company involved. The matter was settled by way of monetary payment to the complainant.
- A private investigator obtained details about a complainant and her post office box from the agency involved in renting the boxes. The agency admitted that the disclosure had been in breach of principle 11 of the Act and, by way of settlement, offered the complainant five years free use of the post office box. The complainant was satisfied with this offer.

TABLE 5: DISCLOSURE COMPLAINTS BY OUTCOME 1997/98

Outcome	Number
Opinion – substance	10
Opinion – no substance	39
Settlement	46
Investigation discontinued	205
	300

Complaints other than access/disclosure

The information privacy principles are concerned with the collection, use and disclosure of information. Individuals obtaining access to information may find that the information is inaccurate and request correction (principle 7). Complaints may arise due to the nature of the information collected (principle 1) or the means by which the information was collected (principle 4). Some agencies are subject to complaints when it appears that they have not taken adequate steps to safeguard the information they hold (principle 5).

Principle 1

- A complainant was asked to fill in an application form to join a club. He complained that the form asked him to provide his date of birth because he did not consider this information was necessary for the purposes of the club. The club explained that while it did not require the date of birth, the information was collected as some benefits

TABLE 6: ALLEGED BREACHES OTHER THAN ACCESS / DISCLOSURE 1997/98

Provision*	Alleged breaches
Principle 1	30
Principle 2	36
Principle 3	39
Principle 4	39
Principle 5	62
Principle 7	25
Principle 8	62
Principle 9	10
Principle 10	23
Principle 12	2

* includes complaints under Health Information Privacy Code 1994

became available to members at a certain age. The club offered to process the complainant's application without him providing an age or date of birth and I discontinued my investigation on that basis.

Principle 4

- A complainant made a claim on his insurance policy and was asked to complete a form giving the insurance company authorisation to pass his claim details to the Claims Register. The complainant understood that if he did not sign this authorisation his claim would not be looked upon favourably. The insurance company explained that as the Claims Register was a new initiative by insurance companies to combat insurance fraud, existing policy holders were to be asked to authorise their claims to be entered onto the Register. New policy holders would be advised at the time the policy was proposed that the insurance company intended to pass all claims to the Register. The insurance company decided to meet the claim and advised me that the form sent to the complainant was an interim measure and had been withdrawn. I discontinued the investigation.

Principle 5

- A complainant's former partner was a bank officer and, when she changed address, her former partner ascertained her new address by

accessing her bank details at work. The bank acknowledged that such actions were not expected from their employees and the complainant did not require any further action to be taken.

Respondents

It would not be safe to look at the number of complaints received against individual agencies and conclude that those agencies must be lacking in Privacy Act compliance. Some agencies will, by the very nature of their dealings with the public and the sensitive information they hold, be subject to more complaints than other agencies. For example, the Department of Social Welfare attracted the most complaints during the year, but it includes agencies such as New Zealand Income Support Service and the Children, Young Persons and their Families Service. It is perhaps not surprising that these agencies would attract a certain number of complaints given the number of people they deal with, the nature of those dealings and the sensitivity of the information they hold and the likelihood of access requests.

One notable feature of Table 7 is the significant gap between the numbers of alleged breaches after the top two respondents (the Department of Social Welfare and the Police) and the other respondents.

It is also interesting to note that the many enquiries I receive do not necessarily translate into complaints. ACC, for example, is subject to many calls to my enquiries hotline but the enquiries made do not translate proportionately into complaints made against the agency. I cannot offer an explanation for this. However, enquirers are encouraged to approach the Privacy Officer of individual agencies to attempt to resolve any matters before they make a complaint to my office. It may be that many potential complaints are resolved in this way. Given the length of time complainants have to wait until I am in a position to investigate their complaints, it is important for agencies to make expeditious and energetic attempts to resolve matters at an early stage.

It is also important to note the outcomes of complaints to the top 11 respondents (Table 8 below), especially where complaints have been settled or where individuals do not require any further action from me. These outcomes indicate a willingness of the organisation to admit fault, where appropriate, and to address the issue to the satisfaction of the complainant.

I attempt to resolve complaints and Table 8 illustrates the success with which my investigating staff implement this policy. Even where I am of the final opinion that the complaint has substance - the agency's actions have amounted to an interference with an individual's privacy - I still attempt to settle the matter at that stage. Of the five complaints

TABLE 7: TOP 11 RESPONDENTS BY ALLEGED BREACHES 1997/98

	Collection	Security	Access	Correction	Accuracy	Retention	Use	Disclosure	Total *
Department of Social Welfare	3	9	39	3	5	1	0	21	81
NZ Police	4	5	40	4	5	0	1	19	78
ACC	19	4	5	0	2	0	2	6	38
Baynet CRA	4	0	6	3	10	4	0	2	29
Department of Corrections	0	1	9	0	1	0	0	3	14
Telecom New Zealand Ltd	0	3	5	0	0	0	2	5	15
Department for Courts	1	1	4	1	1	0	0	6	14
State Insurance	0	1	6	0	1	0	0	2	10
Inland Revenue Department =	2	3	1	0	1	0	1	2	10
Westpac Trust =	1	2	2	0	0	0	0	5	10

* Total number of alleged breaches may exceed the number of complaints received (table 8) as one complainant may allege a number of breaches.
= Equal numbers of complaints received.

TABLE 8: TOP 11 RESPONDENTS BY OUTCOME 1997/98

	Settlement	Investigation discontinued	Opinion – no no substance	Opinion – substance	Other resolution	Other	Total complaints
Department of Social Welfare	10	35	11	1	5	6	68
New Zealand Police	5	41	8	5	0	3	62
ACC	3	13	3	0	1	2	22
Baynet CRA	5	13	2	0	0	0	20
Department of Corrections	0	10	0	0	1	2	13
Telecom New Zealand Ltd	2	5	3	0	1	0	11
Department for Courts	2	5	0	0	2	1	10
State Insurance	2	2	0	1	3	1	9
Inland Revenue Department =	3	3	2	0	0	0	8
Westpac Trust =	4	4	0	0	0	0	8

= Equal numbers of complaints received.

against the Police where I formed the opinion that the complaint had substance, I referred one to the Proceedings Commissioner as I was not able to settle the matter. I would have referred three more but for the fact that the complaints had arisen before all of the remedies became available before the Complaints Review Tribunal.

Complaints Review Tribunal

If my staff have not brought about a settlement, I may refer complaints which in my opinion have substance to the Proceedings Commissioner with a view to instituting civil proceedings before the Complaints Review Tribunal. If I do not do this, I tell complainants of their right to take their own proceedings in the Complaints Review Tribunal.

Last year I referred seven complaints to the Proceedings Commissioner for consideration as to whether civil proceedings should be issued. They remained under consideration by the Proceedings Commissioner at the end of the year.

Eleven complainants commenced proceedings before the Tribunal after:

- I concluded that the complaints did not have substance; or
- I concluded that the complaints had substance and could not be settled but did not refer them to the Proceedings Commissioner for civil proceedings; or
- I discontinued my investigation.

All but three of those complaints were disposed of during the year:

- Four claims were dismissed;
- Two claims were stayed;
- One claim was withdrawn;
- One claim was struck out.

Four cases already before the Complaints Review Tribunal were also concluded:

- One claim was concluded after the Tribunal was satisfied that the defendant had met its obligations;
- Three claims were dismissed.

EDUCATION AND PUBLICITY

Seminars, conferences and workshops

As in previous years, I received a number of requests from agencies for seminars and conference addresses. I attended nine conferences

through the year and gave a number of speeches to other organisations.

The fourth annual Privacy Issues Forum was held in Auckland in July and was attended by 158 people. It attracted a number of international speakers, including Hon Justice Michael Kirby from the High Court of Australia, and was warmly received. I look on the Forum as an important event for New Zealand's privacy community. It brings together people working in the field, from policy analysts and lobbyists, to privacy officers and my own staff. It provides an opportunity to network, to discuss problem issues and to hear about international developments.

As in previous years, I continued to present seminars to newspaper journalists. In these seminars, as well as in answering enquiries from the media, I have given guidance on the proper way to frame official information requests and to identify situations where the Privacy Act is wrongly given as a reason for non-disclosure of personal information.

Twenty-six seminars and workshops were presented during the year by qualified and experienced staff from my office.

The first steps were taken to develop materials for a full day workshop aimed specifically at the mental health sector. Work was not in final form at the end of the year, but the workshop design is to complement the mental health guidance notes and provide clear and practical help to mental health professionals confronting privacy issues.

Printed resources

I continued my practice of releasing compilations of materials produced by my office. Three general compilations were released comprising papers, submissions and speeches. One was dedicated to health issues, and the other two were of a more general nature. I also released a specific compilation of information matching reports.

During the year I released 23 case notes on complaints I had investigated. Work was started on a cumulative index of the case notes issued to date which, when completed, will be a useful resource to people working with privacy on a day to day basis. I expected to publish the index in the first quarter of the new financial year.

The objective of the case notes is to report some of the opinions I have reached on complaints, or to illustrate the types of complaint I received and the approach I took on them. Some record a conclusion I reached for the first time on an interpretation of the Act. In other cases, the application of the law might have been quite straightforward but the principles were being applied to a new set of facts, or in a setting which demonstrated a facet of the application of the Act which may not otherwise have been understood. Other case notes have been issued to

provide a representative illustration of the opinions I have reached.

My case notes are widely distributed to law journals, media, privacy officers and others interested in privacy issues. They are often published in *Private Word* and are available free of charge from my office and on my website.

This year I also released a compilation of decisions of the Complaints Review Tribunal from 1993-1997. As these decisions will not necessarily be reported in law reports, but will have an impact on my approach to complaints, I felt it important for people to be able to access the Tribunal's decisions.

In my last annual report, I mentioned the mental health guidance notes which had been commissioned by the Mental Health Commission. The guidance notes were launched by the Minister of Health in September 1997 and were widely distributed, both by my office and by the Mental Health Commission. I have done two reprints of the guidance notes as demand for them has been high.

The guidance notes are intended to provide clear, accessible and practical help to mental health professionals confronting privacy issues. I intend to revise them from time to time to take account of professionals' experience of working with them. Although the guidance notes appear to have been widely distributed, I am aware that some mental health professionals do not have access to them and are still woefully uninformed about the Privacy Act and other statutes which require or authorise the disclosure of health information. There is a serious need for the Health Funding Authority to ensure that adequate funding is provided to health agencies to undertake training on information matters (especially the Official Information Act) or, if it is doing so, to check the implementation and quality of the delivery of such services.

I have expressed the willingness of my staff to be involved in such training.

In the course of my work on the review of the Privacy Act this year, I released the discussion papers in one volume, four volumes of the submissions I had received, and four subject-specific compilations of submissions. This has enhanced the openness of the process.

Publicity

As in previous years, privacy has maintained a high profile.

Of particular interest during the year were proposals in the health sector for widespread assignment of unique identifiers, which would facilitate tracking of patients through their health transactions. The spectre of centralised health records was of concern to many enquirers to my office,

as was the proposal by the Land Transport Safety Authority to introduce driver licences with digital photographs for uses other than road safety.

The assignment of unique identifiers and collection of health data by health funders arises partly from changes to and the ways in which health services will be delivered in the future. Currently, integrated care and capitation are being mooted as possible directions. Whatever their final form, the proponents of the proposals seem to think they will necessitate the gathering of more information about patients and, possibly, the centralisation of data repositories.

With this is a worrying trend for the funders of health services to collect more and more detailed information about identifiable patients. It is an issue which, while being widely discussed in the health sector amongst the purchasers and providers, is not high in the public consciousness. I am concerned that these issues, which raise significant privacy concerns, have been discussed in a forum from which the consumers of health services have been effectively excluded. In an attempt to find out what was actually happening (as this was not evident), I commissioned a report from Robert Stevens, an Auckland barrister. His report *Medical Records Databases: Just What You Need?* received much media attention and raised public consciousness. Since that report has been issued, the issue seems to have been debated more often in the public arena and I have been invited to comment on proposals at an earlier stage. But I fear there is still a desire to press ahead with unannounced plans and to regard patient opinion as a risk to be managed rather than as a key element of design.

The photo ID driver licence issue received a lot of public attention in early 1998. I have been concerned about this issue since 1995 and I have had much contact with the Land Transport Safety Authority about it over the past few years. I appeared before the Transport Select Committee during its Auckland hearings, and have given numerous interviews on television, radio and to newspapers.

I am concerned that the proposed licence, referred to in more detail later in this report, carries privacy risks which have little to do with driver licensing but much to do with creating the conditions for a de facto national identification card. The Transport Select Committee's report to Parliament and the subsequent debates in the House and in the media will continue to keep this issue in public view.

Newsletter

Private Word, the office newsletter, has continued to be an effective forum to discuss privacy issues and publicise the activities of my office.

Due to increasing demand, the average print run has increased to 5,000 copies. I may have to consider limiting the frequency to curb the increasing costs of production and distribution. It has gone a long way to counter mischievous editorial comment and inaccurate representations of privacy law and practice and the press.

Private Word is available on my website and can be downloaded free of charge. I am happy for *Private Word* to be copied and for the written content to be republished in other magazines providing the source is acknowledged.

ENQUIRIES

Workload

The flow of enquiries accelerated to an average rate of 928 per month. The enquiries team received and answered 10,606 phone enquiries and visits from enquirers. The team also received 535 written enquiries, 429 of which were replied to during the year.

The total number of enquiries was 11,141, which is the highest yearly total yet received and represents a substantial increase of 23% over the previous year. It is clear, however, that in the coming year the service will have to be reduced to remain within the resources available to the Office.

Enquiry topics

As in previous years, enquiries covered a very wide range of topics. However, a few are worthy of mention. A number of people were concerned at the implications of changes to health funding on health information. Some believed the widespread use of unique identifiers and collection of information by health funders to be a threat to patient confidentiality. I anticipate that enquiries on this topic will increase as people become more aware of initiatives in the health sector.

A high proportion of enquiries related to people's rights to request access to their own personal information. Other common enquiries related to the alleged wrongful disclosure of personal information by agencies.

As in previous years, workplace drug testing was the subject of a number of enquiries from both employers and employees. Similarly, the introduction of video surveillance cameras in the workplace was a common enquiry subject. It would appear that some employers are still trying to introduce such practices into the workplace, having given little or no thought to the Privacy Act implications.

Other issues that were the subject of a number of enquiries were:

- Credit reporting
- Telemarketing
- Photo ID driver licences
- Electronic commerce

Frequently, enquiries turned out to relate to the Privacy Act in only a minor way. Many enquiries raised issues which required statutes other than the Privacy Act to be considered. Legislation attracting particular attention included:

- Children, Young Persons and their Families Act 1989
- Health Act 1956
- Rating Powers Act 1988
- Broadcasting (Public Broadcasting Fees) Regulations 1989

The last of these raised some interesting issues. The Broadcasting (Public Broadcasting Fees) Regulations require retailers to provide New Zealand on Air with information about people who have purchased television sets, including their names and addresses. Yet retailers do not seem to be advising purchasers of this disclosure, because many purchasers have called my office after receiving – to their surprise – a bill in the mail from New Zealand on Air.

It is of concern to me that retailers do not seem to be informing their customers that this will happen. Information privacy principle 3 requires agencies to take reasonable steps to inform people of a number of matters, including the intended recipients of the information, when information is collected from them.

Some enquirers asked for the office's comments on new proposals or products or services. The response requested sometimes really required a further understanding of matters other than the Privacy Act. On some of these issues, although assistance was given, it was suggested that legal advice be sought.

Website access for enquiries

The website operated by my office has continued to be a popular means of obtaining information. Fact sheets, case notes, reports on proposed legislation, speeches and *Private Word* are all available on the website.

Work began this year on rebuilding the website. The website contains a huge volume of information, not all of which is easy to find. I decided

to rebuild and restructure it to ensure that information is easily accessible. The new website is expected to be up and running early in the new financial year.

SECTION 54 AUTHORISATIONS

Section 54 allows me to authorise certain actions that would otherwise breach information privacy principles 2, 10 or 11. I am required to consider whether, in the special circumstances of the case, any interference with privacy of an individual that could result from the action in question is outweighed by either:

- the public interest in that action; or
- the clear benefit to the individual concerned which would result from the action in question.

Detailed guidelines are available upon request from my office for any agency considering applying for an authorisation. Three applications for authorisations were carried over from last year, with four new applications this year. Three of the seven remained under consideration at the end of the year.

In one of the completed applications, I was able to suggest alternative means to achieve the same result without breaching the information privacy principles and without my specific authorisation.

I declined two of the applications. In one, I was not satisfied that the action in question would actually breach an information privacy principle. I declined the other application on the basis that the action concerned did not appear to be a one-off action and I was not satisfied that it would, in any case, breach an information privacy principle. I consider that section 54 is only appropriate for one-off actions which are unlikely to recur. If an agency wants to carry out an activity in relation to personal information which would breach one of the privacy principles, the agency would be better to consider asking me to issue a code of practice for that particular activity.

I granted one application.

General Motors New Zealand Ltd

General Motors New Zealand Ltd (Holden) requested an authorisation to allow it to advertise for former employees who were entitled to a deferred pension. Holden is a trustee of the Holden NZ Ltd Pension Plan. Members of the plan who left the company were entitled to elect to receive a lump sum or, in some cases, a deferred or an immediate

pension. Holden did not have current addresses for between 50 and 60 members who were entitled to a deferred pension. The Pension Plan was due to be restructured, which would involve distribution of some surplus to members. The distribution required the consent of all members, which gave Holden another reason for wanting to locate the members for whom it did not have current addresses.

Holden proposed to place advertisements in newspapers in both New Zealand and Australia which would include members' names and last known addresses in the form of suburb and city or town, and the year in which they left Holden's employment.

Section 54(1)(b) allows me to authorise an agency to disclose personal information, even though that disclosure would otherwise be in breach of principle 11, if I am satisfied in the special circumstances of the case that the disclosure involves a clear benefit to the individual concerned that outweighs any interference with the privacy of the individual that could result from the disclosure.

I considered that there was an obvious benefit to the individuals concerned in being alerted to the fact that they had certain entitlements under the Pension Plan. I also saw a benefit in giving members an opportunity to consent to the distribution of the surplus, as it could result in an immediate material gain. I was satisfied that this was a clear benefit to the individuals concerned which outweighed any interference with their privacy which could result from the disclosure.

I granted an authorisation to allow the disclosure on the condition that Holden made reasonable efforts to ensure that information about any member who was located would be removed from the text of the advertisement and notice before they were next placed or sent. I further required that the disclosure be made only once Holden had taken certain specified steps, which would not involve publication, to trace members.

LEGISLATION

One of my functions is to examine any proposed legislation which may affect the privacy of individuals and to report to the Minister of Justice the results of that examination. During the year I submitted nine formal reports to the Minister on bills before Parliament. These reports are available from my office and are posted on my website. They are often followed up with an appearance before a select committee.

The Cabinet Office Manual requires departments to signify compliance with the information privacy principles, the public register privacy principles, and the information matching guidelines when seeking introduction of a bill into Parliament or when proposing the issue of

regulations. Accordingly, I am frequently consulted by departments concerning new proposals. I also make submissions to bodies such as the Law Commission when particular laws are under review.

I mention below a selection of the legislative matters upon which I commented during the year.

Companies Act 1993

The Companies Act 1993 introduced a new requirement for companies to publish details in their annual reports of executive remuneration exceeding $100,000. As existing companies were re-registered I was contacted by a number of people in the corporate sector expressing concern as to the effect of the law on their privacy and I concluded that the matter warranted review.

I have become acutely aware in my role as Privacy Commissioner of the sensitivity which many New Zealanders accord details of their income. New Zealanders do not wish other people to know their wages, salaries or other incomes without their say-so. Clearly there are some people who are quite happy for some of their income details to be known and this is quite consistent with notions of personal privacy since it is their right to be open about their income if they so choose. However, it does not follow that their lack of concern on the issue should dictate how others preserve their privacy.

There is undoubtedly a legitimate role for publication of remuneration of *directors*. I support the requirement to publish full details of remuneration of directors including, in relation to executive directors, details of all remuneration from a company, not simply directors' fees. Directors must be accountable to shareholders. However, *employees* are usually seen in a somewhat different light, owing their accountability to the chief executive and directors, and not directly to the shareholders.

In November 1997, I reported to the Minister of Justice that the mandatory publication of executive remuneration is detrimental to individual privacy and that, if a scheme was considered necessary, a substitute scheme could be devised which better accorded with privacy.

My report canvassed the existing requirements and the privacy issues in disclosure of remuneration details. I highlighted what I believed to be the shortcomings of the present provision and outlined elements of a disclosure regime which would respect privacy. Any reform should, in my view, require:

- a clear identification of the objectives of the publication of remuneration details, for those objectives to be balanced against the

loss of privacy (if any), and for any regime to be drafted so that the infringement is no more intrusive on privacy than it need be (a proportionality test);

- that the regime, as far as possible, aggregate information so details of individual remuneration cannot be identified (this might require simply the report of global figures following a particular formula or by using much wider bands than are presently used);
- where it might be anticipated that a single individual's remuneration will be identifiable, the mechanism for generalising the details (such as banding) be such that the actual figure cannot be determined from published details closer than 20%;
- the disclosure of the average movement of such remuneration compared with previous years.

The Minister of Justice copied my report to the Minister of Commerce who has responsibility for the Companies Act. The Minister directed his officials to assess how a review of the mandatory disclosure of executive remuneration might be worked into the programme for on-going review of company law.

Evidence (Witness Anonymity) Amendment Bill

During the year I was consulted by the Ministry of Justice on the preparation of a bill to protect witnesses in criminal proceedings by extending the existing powers of courts to suppress the identity of witnesses. After the bill's introduction into Parliament I made a report to the Minister of Justice supporting the measure.

I considered the possible effects on privacy of:

- witnesses and their families; and
- accused persons.

The bill would enhance privacy interests of witnesses and their families. It would allow the control of disclosure of personal information in circumstances where it could lead to harm to a witness or his or her family or property. On previous occasions, such as my report on the Domestic Violence Bill, I had noted the links between freedom from violence and the ability to exercise individual autonomy and enjoy personal privacy.

With respect to the accused person, the bill would limit the right to have access to certain personal information which would usually be available pursuant to access rights under the Privacy Act. However, the right of access is not absolute and there are a variety of existing grounds for withholding information including where the disclosure of the

information would be "likely to endanger the safety of any individual". I took this into account, and the special safeguards in the bill, in concluding that any perceived limitation on current rights of access to information was reasonable.

Health Occupational Registration Acts Amendment Bill

The eleven health occupational registration statutes affected by this bill each contain registers of persons permitted to work within a particular health-related profession or occupation. I recommended to the Minister of Justice that the opportunity be taken to create each of the statutory registers as "public registers" for the purposes of the Privacy Act by adding them to the Act's Second Schedule.

This bill was introduced into Parliament at a time when I was examining a variety of public register issues in the review of the operation of the Privacy Act. In particular, I had been studying the position of those statutory registers which are open to public search but are not listed in the Second Schedule. There are more than 150 such registers. In the course of my review, I sought the opinion of the Ministry of Justice which confirmed my view that there were no reasons to exclude these statutory registers from the Schedule. It now appears appropriate to start bringing such registers into the Privacy Act public register regime.

The Minister copied my report to the select committee. I also showed the report to the agencies maintaining the health registration statutes. Several agencies contacted my office to indicate they supported the proposal. The select committee reported back on the bill towards the end of the year but, for various reasons, did not act on my recommendations. There was some concern as to whether the bill was the appropriate legislative vehicle for making such change. Consideration will likely be given in the new year to creating the registers as "public registers" by Order in Council.

Human Assisted Reproductive Technology Bill

During the year the Human Assisted Reproductive Technology Bill remained before a select committee. Amongst other things, the bill would create new databases of information about donors of gametes (sperm or ova) and confer rights on children born as a result of ART to find out about their biological origins. The bill touched upon issues which I had been considering for some time through discussions with the Ministerial Committee on Assisted Reproductive Technology and the officials committee which reviewed the MCART recommendations.

Although I supported legislation to regulate the issues, I had some misgivings about the bill. For example, it did not set out the particulars which would have to be retained on the centralised records system. Nor did the bill establish a procedure, such as a complaints mechanism, for ensuring that rights of access and constraints on disclosure would be exercised as intended.

I was aware that the Government intended to introduce its own legislation on the subject. Given my limited resources and desire to use them to best effect, I chose not to prepare a report in respect of the member's bill and instead awaited the Government bill, which was expected to be introduced into Parliament shortly after the end of the year.

Interpretation Bill

The Interpretation Bill will replace the Acts Interpretation Act 1924, which is the main guide to statutory interpretation in New Zealand. I submitted a report to the Minister of Justice supporting the provision in the bill which made it clear that it would apply, not only to statutes and regulations, but also to other forms of delegated legislation such as codes of practice issued under the Privacy Act. The earlier Act did not extend to codes of practice, which were unknown in 1924. Benefit will accrue from the new bill, as it has been difficult to ensure consistent and appropriate rules for interpretation of codes of practice without relying on the 1924 Act. Complications could arise if the 1924 Act applied to the interpretation of the information privacy principles in the Act but not to a modified set of principles contained in a code. The bill remained before a select committee at the end of the year.

Land Transport Bill

The Land Transport Bill will consolidate and modernise transport legislation. The controversial aspect from a privacy perspective was the proposal to change from the present paper lifetime licence to a ten year renewable credit card sized licence bearing a digitised photograph. The implications of the proposal were so profound in privacy terms that I urged the Land Transport Safety Authority (LTSA) to undertake a thorough privacy impact assessment which would properly describe and evaluate the proposal, and alternatives, in privacy terms so that an informed decision could be taken. Unfortunately, a suitable privacy impact assessment was not prepared or produced publicly at an appropriate time to inform the public or decision makers on the matter. Indeed, a privacy impact assessment by the LTSA in an initial form was prepared quite late in the policy formulation process to coincide with a

government decision to proceed with a photo ID driver licence. It caused me considerable concern that the LTSA frequently referred to public opinion surveyed without making the privacy issues available to respondents.

My principal concern was the proposal to oblige drivers to carry the licence at all times while driving, meaning, in effect, that most adults would have to carry their licences at all times. This would provide ideal conditions for government agencies, police officers, retailers and other businesses to ask for the card as standard identification in a variety of dealings unrelated to road safety. Indeed, the provision in the bill to issue proof of identity cards to non-drivers confirmed my view that there was a deliberate desire to create the conditions for a state-backed identity card without calling it this in so many words. If New Zealand is to adopt a national ID card it should be a conscious decision following an informed public debate, not an incidental consequence of road safety legislation.

I participated in public debate on the proposal and appeared before the select committee studying the bill. I remained unconvinced as to the road safety merits of this hugely expensive project. It would be a significant imposition on many hundreds of thousands of law-abiding licensed motorists to tackle a problem limited to a much smaller group of unlicensed or disqualified drivers. Yet it has not been made clear how the compulsory carrying of a licence by all drivers will affect that latter group, since they already drive in the knowledge that they are breaking the law. One cannot but suspect that random stopping or road-blocks to check driver licences will be the eventual and inevitable outcome.

A good deal of the reporting of my position on the photo ID driver licence wrongly characterised it as outright opposition. I publicly queried whether a case had been made for the proposal based upon the significant costs to privacy but was open to be persuaded. A proper justification should have been demanded by anybody given the financial costs, which I calculated to be in the region of $135 million in licence fees alone - with every driver having to pay a further fee every ten years. However, given the LTSA's attitude, I resigned myself to what appeared to be the inevitable introduction of the new licence and the detail of my report was based upon an assumption that there would be a photo ID driver licence.

Even on that basis there were plenty of issues. I raised questions on such matters as who might have access to the computer database of photographs of practically all adult New Zealanders. I questioned the need to impose a mandatory obligation to carry the licence at all times. The powers to detain drivers applied whether or not a card was carried, so there appeared to be little benefit in the photograph on the licence. I

also suggested that the penalties to be imposed upon otherwise licensed and lawful drivers who failed to hold the licence when stopped by an official seemed oppressive. My report to the Minister of Justice in March 1998 made six particular points:

- individuals should not have to pay for heightened state surveillance;
- individuals should not be obliged to carry identification documentation;
- the Police should not be given the power to detain individuals for identity checks;
- the bill should secure the digital photographs against uses unconnected with road traffic enforcement;
- the display of date of birth on the card should be voluntary;
- the bill should not establish the LTSA as a purveyor of ID cards.

The bill had not been reported back from the select committee at the end of the year. It was expected to be enacted late in 1998.

Privacy Act: Fifth Schedule

Key law enforcement agencies have for many years shared a law enforcement system formerly known as the Wanganui Computer. The Wanganui Computer was organised so that each category of information held was identified as the responsibility of a named agency and other law enforcement agencies needing the information were given rights to access it on-line. The Wanganui Computer Centre Act 1976, which governed such arrangements, was repealed with the enactment of the Privacy Act 1993 but the Fifth Schedule continued the sharing arrangements. There has been some change in the Fifth Schedule over the years as the sector has been restructured and information sharing needs have changed. During a transitional period, amendments could be made by Order in Council. The Privacy (Fifth Schedule) Order 1997, which came into effect at the end of the 1996/97 year, replaced the entire schedule with the one currently in force. With the end of the transitional arrangements amendments may now only be made by statute.

During the year, the Privacy Amendment Act 1998 made a small change to the Fifth Schedule. The amendment added to the description of police records an item relating to firearms licences which concerned the particulars of persons authorised to posses firearms in accordance with the Arms Act 1983. The new entry allowed the Department for Courts to have access to that information. Access is limited to identity details of persons who possess firearms where that information is required for the purpose of serving protection orders made under the Domestic

Violence Act 1995. Prior to the passage of the Domestic Violence Act 1995 firearms confiscation was not a standard condition in respect of persons served with orders. However, under the Domestic Violence Act firearms may be confiscated where the appropriate orders are served. While bailiffs generally serve orders on defendants, in cases involving firearms it is desirable for the police to serve the orders. Hence the Department's need to access firearms licence records.

Radiocommunications Amendment Bill

The bill proposed to put the national frequency register on a statutory basis and combine it with the register of radio frequencies. The Ministry also sought to establish a more satisfactory legislative basis for protecting privacy and enable a generally freer flow of authorised information from the register to groups representing amateur radio operators. I supported the approach the Ministry had taken and in a report on the bill to the Minister of Justice I discussed certain key provisions which:

- specified the purpose for which the register is kept;
- specified the search references for searching the register;
- outlined the purpose for which the register may be searched; and
- protected the residential addresses of natural persons.

The bill remained before a select committee at the end of the year. It is a particularly interesting initiative as it is the first to allow people to elect to have their details released to requesters. The main shortcoming, in my view, was that the bill did not provide that the relevant sections be listed in the Second Schedule to the Privacy Act as "public register provisions". I recommended that it should.

The other aspect of interest in the bill concerned the creation of a new statutory offence to make use of, to reproduce, or to disclose the existence of, a radiocommunication which was not intended for the recipient. The new offence is intended to protect the privacy of radiocommunications and I supported the measure. It has particular relevance to the undesirable practice of "scanning" private cellular and cordless telephone calls.

Taxation (Remedial Provisions) Bill 1997

The use of the tax file number (popularly known as "the IRD number") is a matter of some importance in privacy terms. As a number assigned by the Government to practically all adult New Zealanders, its potential as a national identification number raises privacy concerns. These privacy concerns are increased because the number is used as a personal identifier

for tax records. Tax records are considered to be very sensitive in our society as they contain, amongst other things, details of wealth, income, expenses and relationships. The use of the tax file number by organisations other than the IRD itself is a matter of concern, and is also related to concerns about information matching, data linkage and profiling.

The tax file number was originally created for income tax purposes. It was later brought into operation in respect of the Goods and Services Tax introduced in 1985. The bill would formally align the GST Act with other taxation legislation to make it clear that the tax file number is the unique identifier to be used by IRD for both GST and income tax purposes. This would bring the law into line with existing departmental practice.

One privacy concern with present departmental practice was highlighted. The issue arises in respect of sole traders in business and individuals. Traders are required to publish their GST number on invoices. Accordingly, sole traders are required to publish their personal tax file number on their invoices. Some sole traders have, over the last few years, contacted me to express concern about this practice which they believe risks their financial privacy or the security of their personal information. A number have been concerned at third parties having easy access to their tax file number.

In a report to the Minister on the bill I suggested that the IRD consider the feasibility of enabling concerned sole traders to have a separate GST number issued to them if they wished. Of course, IRD would still be able to link internally the records from that GST number to the individual's other tax records referenced by the tax file number. The bill was enacted without adopting my suggestions. However, my report was referred to the Department for further consideration.

Telecommunications Amendment Act 1997

This amendment was a late addition to the package of measures contained in the Harassment and Criminal Associations Bill. While the bill could generally be characterised as a major extension of the powers of interception to the detriment of privacy, I considered this initiative brought some benefit. I was consulted on the proposal prior to its introduction and formally reported to the Minister on the matter in September 1997.

The proposal related to the use of telephone analysers, which are devices that can be attached to a telephone line to enable the recording of data generated as a result of telecommunications made using the line. The data recorded, such as the number called and the time and duration of the call, does not include the content of the communication.

The use of telephone analysers raises privacy concerns. Since the call data collected by the analysers is "personal information" about the subscriber or caller, the use of analysers for collecting personal information and the use and disclosure of the information collected is subject to the information privacy principles. Nonetheless, this does not adequately dispel the privacy concerns since the existence of "maintenance of the law" exceptions leaves the matter unclear and largely determined by the attitudes and policies of private telephone companies and law enforcement authorities.

The measure placed the attachment of telephone analysers on a firm statutory basis which involved:

- a general prohibition on the attachment of telephone analysers except for certain limited purposes with the agreement of the network operator, primarily relating to the maintenance of the network and the investigation of offences; and
- a requirement for the Police or New Zealand Customs Service to obtain a "call data warrant" before utilising a telephone analyser.

I supported the proposal as it seemed an appropriate and traditional way of resolving the competing public interests relating to privacy and maintenance of the law. The requirement to obtain a judicial warrant means that an independent person is required to consider whether the circumstances justified the attachment of a telephone analyser. This is preferable to the previous position whereby such decisions were informally agreed between two parties, the Police and network operator, neither of whom could be characterised as disinterested. Privacy and public accountability are further enhanced by a requirement to report to Parliament on the number of warrants granted.

INTERNATIONAL DIMENSION

Today we live in an "information society". Technology has removed many previous technical barriers to the free flow of information between people, computers, agencies and nations. Meanwhile, increased globalisation in commerce has led to interconnecting social and economic networks in which people and places are linked by the flow of information and money.

The international dimension is central to the Privacy Act. The Act gives effect to New Zealand's obligations under the International Covenant on Civil and Political Rights. It is also a reaction to concerns about the risks posed to privacy by computer databanks and other accoutrements of the perceived surveillance society. Finally, it is a direct outcome of the OECD's efforts to harmonise the laws of developed trading

nations to avoid unnecessary impediments to transborder flows of personal data.

Much could be said about the international dimension of the year in review but I will focus only on two aspects.

EU Directive on Data Protection

No-one interested in the protection of privacy in the 1990s can fail to be aware of the significance of the European Union Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (the EU Directive). The 15 EU States have now had three years to implement the 1995 Directive in national law and some will have done so by the deadline of October 1998.

New Zealand is not a member of the European Union and is not bound by EU Directives. However, we share many of our values with the democratic states of Europe. Furthermore, the EU is a powerful and affluent trading bloc whose standards cannot be ignored by a small country like New Zealand. Most relevant in this respect are the data export controls which will be imposed by EU countries from October on transfers of personal data to "third countries" which do not provide "adequate protection" to such data.

New Zealand, through the far-sighted enactment of the broadly-based Privacy Act, is in a fortunate position with respect to the EU Directive. New Zealand business in general can be relatively sure that the implementation of the Directive will not impede our commerce. Similarly, when European businesses and governments transmit personal data to New Zealand for processing, they can be confident in the knowledge that the Privacy Act provides adequate legal protection to the information. Businesses in other third countries cannot operate with such certainty.

I have been somewhat disappointed that businesses and government agencies which potentially benefit from our law do not seem to have fully appreciated the matter. New Zealand presently is in a position of comparative advantage, shared in our region only by Hong Kong - a jurisdiction which understands the desirability of acting to avoid impediments to its international trade. I am unaware of businesses overtly marketing the advantage of using New Zealand to process data. The comparative advantage may not last for very much longer as other jurisdictions legislate to bring privacy law to their private sectors.

During the year I examined the implications of the EU Directive for our law in my first review of the operation of the Privacy Act. I am confident that the Act generally offers adequate protection, but will make some recommendations for amendment to address some particular

concerns which have been uncovered. Meanwhile, I will continue to keep the European Data Protection Commissioners informed about our law and practice, as they are accorded a special role under the EU Directive to provide advisory opinions on the adequacy of the privacy protections in third countries.

Regional cooperation

Most countries of our type have data protection or information privacy protection laws. All EU countries, and most other European countries, have broadly-based data protection laws which cover both the public and private sectors. Outside Europe, this model also exists in Quebec and Hong Kong. Canada and Australia have federal privacy laws and a mix of state and provincial privacy laws, supplemented by sectoral laws covering matters such as credit reporting. Both countries are developing privacy standards for the private sector. Coverage of privacy law in the USA is patchy, with a number of sectoral laws supplementing the Federal Privacy Act of 1974.

Around the Pacific Rim there are information privacy laws, policies or agencies of various sorts in at least the following jurisdictions:

- Commonwealth of Australia;
- Australian States of New South Wales and South Australia;
- Hong Kong Special Administrative Region;
- Taiwan;
- South Korea;
- Russian Federation;
- Dominion of Canada;
- All Canadian provinces and territories;
- United States of America;
- State of Hawaii.

There are also sectoral laws in various jurisdictions, such as a medical records privacy law passed in 1997 in the Australian Capital Territories.

The EU Directive means that the adequacy of the privacy laws in our region will be scrutinised over the next few years. Canada, Australia and the USA have for a number of years been studying what response, if any, is appropriate for them. Others in our region seem to have been biding their time in announcing any response. However, I understand that Singapore and Malaysia are now considering adopting information privacy laws.

There has been little discussion so far on the effect of the EU Directive

on developing countries. With the financial assistance of the Ministry of Foreign Affairs and Trade, I was able to play a small part in fostering an understanding of the implications by bringing officials from India, the Philippines, Western Samoa and Papua New Guinea to the Privacy Issues Forum and the associated meeting of Privacy Agencies of New Zealand and Australia (PANZA). Naturally, a law of the New Zealand type may not suit these widely varying jurisdictions. However, I was assured by the participants that they welcomed being informed on the New Zealand model and the opportunity to study the approaches taken in Australia and Hong Kong.

The PANZA meeting held in Auckland in 1997 also gave an opportunity to discuss the state of privacy protection in our region. The Hong Kong Privacy Commissioner for Personal Data gave a presentation on the position in several Asian countries. The subsequent PANZA meeting held in Sydney in 1998 was also enhanced by the participation of the Hong Kong Deputy Commissioner and a standing invitation has been issued for future participation.

In April 1998 the Hong Kong Privacy Commissioner convened the First Asia-Pacific Forum on Privacy and Data Protection to which Privacy Commissioners and appropriate officials in various jurisdictions were invited. This very successful meeting was held in conjunction with the 23rd meeting of the International Working Group on Data Protection in Telecommunications. The latter meeting brought together a variety of European and North American experts who were able to share their experiences and knowledge with the participants from the Asia-Pacific region. Once again, I was grateful that the Ministry of Foreign Affairs and Trade was able to facilitate the participation of the Papua New Guinea Attorney-General in those meetings.

PUBLIC REGISTERS

Part VII of the Act establishes four public register privacy principles, provides for the issue of public register codes of practice and establishes a complaints jurisdiction. I have a remit to monitor compliance with the public register privacy principles and keep them under review. Public register issues also arise in my work of examining legislative proposals for their effect on privacy.

The public register privacy principles are not drawn directly from the OECD guidelines. Nor do they have any precedent in overseas legislation. The principles are an original attempt to address the difficult privacy issues arising from the establishment of statutory registers which are open for public search.

All countries with privacy laws have wrestled with the difficulties in preserving privacy while establishing and operating public registers. Some jurisdictions have concentrated on crafting privacy sensitive regimes in relation to particular registers. The New Zealand approach has been to try to address the problem in a principled way based upon the nature of open registers rather than addressing each register on a case-by-case basis. However, our law allows for case-by-case tailoring of privacy protection through the legislation establishing the register or a Privacy Act code of practice.

Second Schedule list of public register provisions

The Second Schedule to the Privacy Act lists all those statutory provisions which have been declared to be "public register provisions" for the purposes of the Privacy Act. The public register privacy principles apply only to those registers maintained pursuant to the provisions listed in the Schedule. A review of all relevant legislation to see which other registers might appropriately be added to the list has not yet been undertaken. Accordingly, the Schedule lists only those considered by the Select Committee when the Privacy Act 1993 was enacted, plus some which have since been added. When I examine legislation creating new registers, I often recommend that the responsible department consider whether the relevant provisions should be listed in the Second Schedule.

No further public register provisions were added to the Second Schedule this year. However, I recommended to the Minister of Justice in a report on the Radiocommunications Amendment Bill that the register of radio frequencies should be declared to be a public register for the purposes of the Privacy Act. The bill contained several innovative features which I supported, most notably:

- a statement of purposes relating to the right of public search to the register; and
- an ability for licence holders to *opt into* the release of details for non-statutory purposes, which related to a desire to allow address lists to be released to associations representing amateur operators.

The bill remained before a select committee at the end of the year.

Suppression of details on public registers

The enactment of the Domestic Violence Act 1995 was an important development affecting a broad range of public registers. The Act enables people who obtain a protection order to apply to the agencies administering certain public registers for a direction that information on

the register likely to disclose the person's whereabouts not be made available to the public where that would prejudice the person's safety. Where an application is declined the applicant may complain to the Privacy Commissioner, and the details will be suppressed until the complaint is dealt with.

The importance of the Domestic Violence Act is that, like the public register privacy principles themselves, it addresses privacy issues arising from the operation of public registers in a broadly based way rather than focusing on a single public register.

In my 1997 report on the Harassment and Criminal Associations Bill I recommended that a similar approach be considered for people who obtain a restraining order in relation to acts of harassment. The Justice and Law Reform Committee reported:

> "The Privacy Commissioner expressed concern that victims who apply for restraining orders need their privacy protected, especially their home address and phone number. These details can be disclosed on public registers such as those under the Electoral and Births, Deaths, and Marriages Registration Acts.
>
> "Section 115 of the Electoral Act 1993 allows the Chief Registrar to direct that a person's name not be included on the electoral roll where publication would be prejudicial to his or her personal safety. Where a protection order under the DVA is enforced it is sufficient to produce the order, without having to produce any further evidence. The proposed restraining orders under the provisions in the Bill have a similar effect. Therefore, we recommend a new clause to amend the Electoral Act 1993 so that a restraining order made under the provisions in the Bill will be sufficient to justify the protected person's name being placed on the unpublished roll.
>
> "We note that the Privacy Commissioner suggested adapting Part VI of the DVA to enable people who obtain restraining orders to get directions that their personal details contained in public registers be held in a confidential list. We understand that as part of the Privacy Commissioner's review of the Privacy Act 1993, a discussion paper will be released in the near future relating to the public register provisions in the DVA. The discussion paper may make a recommendation that will affect Part VI of the DVA. Therefore, it seems preferable to *defer the decision* of incorporating a regime similar to that in the DVA until the outcome of the discussion paper is known. We consider it a preferable alternative to recommend the *interim measure* as outlined above." [Emphasis added]

I took the select committee's comments to indicate that the members saw the amendment to the Electoral Act as an interim measure pending consideration of the merits and workability of some broader means to suppress details of persons who obtain a restraining order. As part of my

review of the Privacy Act I released a discussion paper touching on the issue and, as a result of studying the matter and submissions, expect to offer an appropriate recommendation in my report due after the end of the year.

Electoral roll

Anticipating a review of electoral law following the 1996 election, I examined aspects of the Electoral Act which raised privacy issues and reported to the Minister of Justice early in 1997. The electoral roll is the key administrative tool for the conduct of elections and most of the comments in my report were directed to it. The electoral roll is one of the most important public registers listed in the Second Schedule covering, as it does, almost the entire adult population of New Zealand.

My report questioned the continuing need to collect occupation details since it appeared that they are of little use in the administration of elections but, once published, are available for non-electoral purposes. The main electoral value of occupational details seemed to lie in enabling parties to target their political information, so it seemed appropriate to me to make the supply of this information voluntary.

An alternative would be to make occupation available only to approved persons, such as political parties and researchers, but not to include them on the published roll. The Electoral Law Committee's report noted the concern but, disappointingly, did not explain its recommendation that provision of occupational details should continue to be compulsory.

Each electoral roll is reformated into a "habitation index" in which the names of electors are shown under the numbers and addresses of the streets or, in country areas, the localities in which they are shown to be currently registered. The result is a roll which clearly indicates the names of electors registered in each dwelling. The habitation index was introduced in 1981 to enhance electoral administration and has a valuable, and very proper, role in administering elections, also enabling political party canvassers to carry out roll checks and house calls.

My concern related to the sale of the habitation index for non-electoral purposes. Regulations allow for the sale of the habitation index at $30 for those needing it for electoral purposes and at $100 for people with no such relevant purpose. The result is that information collected by compulsion of law, which must be published for electoral purposes, can be reformated and sold without any limitation as to purpose. This is quite at variance with the approach of the information privacy principles, so I was pleased that the Electoral Law Committee recommended that the sale of habitation indexes for non-electoral purposes be discontinued.

Using public registers for direct marketing

A constant refrain in letters to my office, and in submissions received in consultation on the review of the Act, is serious concern at the release of bulk information from registers for commercial use - primarily direct marketing. Concerns have been expressed to me not only by individuals and community groups but also by the agencies maintaining public registers themselves.

Certain registers have been revealed as having a commercial value and are subject to constant and continuing requests for bulk data which is used to create and sell direct marketing lists. For example, householders erecting or altering a building must apply to their territorial authority for a building consent. Councils create weekly or monthly lists of the applications received, which are regularly requested by commercial interests. As a result, people who have applied for consents receive, out of the blue, solicitations from companies they have never dealt with entreating them to purchase building supplies, products or services. They have been given no choice in this.

Similar issues arise in respect of the use of valuation rolls and rate records. For instance, in June 1998 it was revealed that thousands of Auckland valuation records had been sold to a marketing company in Queensland, a jurisdiction without privacy laws. In the first wave of marketing, Auckland property owners received letters inviting them to refinance their mortgages. This raised both privacy and consumer protection concerns.

I hope to offer recommendations on this problem in my report on the review of the operation of the Privacy Act. However, during the year there were two promising developments in relation to the issue. The first concerned the Radiocommunications Amendment Bill which, as already mentioned, adopted the novel approach of allowing individuals to *opt into* certain secondary uses of register information. This means, for example, that radio licence holders who do not wish to have their details shared with clubs representing radio amateurs are able to authorise this.

The second development followed quite quickly upon the publicity arising from the mass sale of valuation data to the Queensland marketing company. The select committee then studying the Rating Valuations Bill included a new provision which will enable regulations to prescribe limitations or prohibitions on the bulk provision of district valuation roll information for purposes outside the purposes of rating legislation.

I continue to follow such initiatives with interest.

FUNCTIONS UNDER OTHER ENACTMENTS

Occasionally I am required to exercise and perform functions, powers

and duties which are conferred or imposed on me by other enactments. These statutory provisions tend to be of four types:

- complaint mechanisms;
- requirements for my approval of agreements;
- obligations to consult with me; and
- my appointment to other bodies.

Complaints under other legislation

Although comparatively few complaints were received under my alternative complaints jurisdictions, each fulfilled an important check on the exercise of particular statutory provisions. The mere existence of a right to complain about the effect on privacy of the exercise of another statutory function can lead to additional care being taken by statutory officials in the exercise of those powers, including the development of processes and safeguards to ensure that complaints do not arise.

I am empowered to receive complaints under section 22F of the Health Act 1956 about a failure or refusal to transfer health records between health agencies or to an individual's representative. This function was discussed in more detail in an earlier annual report. Four complaints were resolved during the period. Two were settled and one was discontinued without my needing to form an opinion. I formed the opinion that one complaint had substance.

Part VI of the Domestic Violence Act gives me the jurisdiction to investigate complaints against refusals by registrars to suppress residential details on certain public registers following an application from someone who has a protection order and fears for his or her personal safety if those details were to be released. I did not receive any complaints this year.

Section 11B of the Social Security Act 1964 provides that a person may complain to the Privacy Commissioner about a breach of the code of conduct issued by the Director-General of Social Welfare under that section. Part VIII of the Privacy Act applies to such complaints as if the code of conduct were a code of practice under the Privacy Act. The code of conduct governs demands by the Department of Social Welfare to supply information or documents about beneficiaries under section 11. The first such code came into force on 17 December 1997. I did not receive any complaints during the year.

Approval of agreements

Section 35 of the Passports Act requires the Privacy Commissioner's

approval to be obtained in relation to agreements for the supply of information from the passports database by the Department of Internal Affairs to the New Zealand Customs Service. My approval is also required for any changes to that agreement. No agreements have been approved to date, although my office made comments on a draft agreement during the year. I understand that information has been supplied, and continues to be supplied, without any agreement approved by me.

Similarly, section 26 of the Passports Act requires the Privacy Commissioner's approval to be obtained in relation to agreements for the supply of information from the New Zealand database to Australia. I have not approved any agreements or changes to any existing agreements during the year.

However, an agreement was signed in late 1995 between the Secretary of Internal Affairs and the Secretary of the Department of Immigration and Ethnic Affairs of Australia. My approval was not sought, although it is required. During the year my office commented on that agreement, suggesting a number of changes. I understand that information has been supplied, and continues to be supplied, pursuant to the 1995 agreement notwithstanding that I have not approved it and that I am unlikely to approve it in its current form.

I regard as serious the fact that information from the passports database continues to be supplied in the absence of the approvals required by sections 35 and 36 of the Passports Act.

Consultations

Other statutory officers have, on occasion, to form a view on matters which have a bearing on privacy. Some statutes require officers to consult with me on relevant matters.

Both the Privacy Act and the Health and Disability Commissioner Act anticipate consultations between the two Commissioners on appropriate complaints. Complaints may be referred from one Commissioner to the other where more properly dealt with under the other jurisdiction. Consultations on the transfer of complaints are dealt with on an informal basis and no separate records are kept.

The Customs and Excise Act 1996 requires the Chief Executive of the New Zealand Customs Service to consult with the Privacy Commissioner in relation to agreements with overseas law enforcement and customs agencies governing disclosure of information. Consultation was commenced in relation to one agreement.

The Financial Transactions Reporting Act 1996 came into force during the year. It requires the Commissioner of Police to consult with me in

respect of the preparation of suspicious transaction reporting guidelines. No consultations occurred during the year, although I understand that the Police are developing a set of guidelines for law practitioners, on which consultation will follow next year.

Section 11B of the Social Security Act (as amended in 1997) provides for a code of conduct to be issued by the Director-General of Social Welfare in consultation with the Privacy Commissioner. The code governs demands made by the Department of Social Welfare under section 11 for information or documents about beneficiaries. The need for the code of conduct was identified by the Parliamentary Inquiry into the Privilege Provisions of section 11 of the Social Security Act undertaken by the Social Services Committee in 1994. This arose from public concern about approaches made to educational and medical institutions by Income Support officers seeking sensitive information about beneficiaries.

As there was limited opportunity for consultation before the first code of conduct came into force on 17 December 1997, the Department agreed to my suggestion that a clause requiring a review of the code after one year be included in the code. I hope that, in the review, the Department will fully consult with groups representing beneficiaries and agencies likely to be the subject of section 11 requests, such as the Bankers' Association.

The Official Information Act 1982 and the Local Government Official Information and Meetings Act 1987 require the Ombudsmen to consult with the Privacy Commissioner in relation to review of official information access requests where privacy is a possible ground for withholding information. During the year 77 formal consultations under the two Acts were completed.

TABLE 9: CONSULTATIONS WITH THE OMBUDSMEN 1993-98

Number of consultations	
1993/94	22
1994/95	26
1995/96	60
1996/97	87
1997/98	77

I have seen my role to endeavour to "add value" to the work of the Ombudsmen in reviewing the withholding of information under the freedom of information legislation. In some cases I agree with the Ombudsman's preliminary assessment. In many cases, my comments

and suggestions have been in whole or part adopted by the Ombudsman in his final opinion. My role is a consultative one and I do not see it as a narrowly advocating only a privacy viewpoint.

Several cases over the past year have required me to consider whether adults who have been adopted should be able to access information about their natural parents and siblings. These cases have sometimes arisen after the natural parents' death and have sometimes arisen in a context where there has been contact between the natural parents and the adult requester.

The complexity of these cases has been compounded by the regime of secrecy which governed adoptions prior to 1985, when the Adult Adoption Information Act came into force. In some cases, requesters have attempted to find the names of their birth fathers when this information was not on their birth certificates, which meant the Adult Adoption Information Act prevented their obtaining this information. The Adult Adoption Information Act overrode both the Privacy Act and the Official Information Act in this context.

Under the old regime the court records were subject to a statutory requirement of confidentiality. Some requesters asked for information from the Department of Social Welfare's records, which often closely mirrored the court's records. In those cases, the Ombudsman and I concluded that any information identifying the parents or siblings should be withheld. Releasing information which is, to all intents and purposes, identical to the information on the court records would undermine the statutory requirement to keep the court records confidential.

The Ombudsmen and I appreciated the difficulty faced by adult requesters who had a legitimate reason for seeking access to information which would enable them to identify close family members, because they did not have any lawful means of doing so. While this group may be relatively small in terms of numbers, they have a significant human need for information about their families of origin which cannot be addressed in the framework of the current legislative provisions for access to adoption information. Statutory reform seems desirable.

In another consultation, an adult requester asked Social Welfare for information about her natural mother, who had been fostered as a child. The requester's adopting parents and mother had died and the information dated back to early this century. I advised the Ombudsman that I did not consider it was necessary to withhold the information to protect privacy in this case. I took into account the age of the material and the fact that the subjects of the information had either consented to the release or had died. While the information was of a fairly superficial nature, I considered it would give the requester some insight into the life of her natural mother as a child.

Participation on other bodies

Pursuant to the Human Rights Act 1993 I am, by virtue of my appointment as Privacy Commissioner, also a Human Rights Commissioner. As such, I participate in the meetings of the Human Rights Commission. I attended six formal meetings of the Commission during the year. During the year I was Acting Proceedings Commissioner on a matter concerning proceedings brought against a bus company when the Proceedings Commissioner was unable to act. With additional time involved as a non-executive Commissioner with consultations and discussions, this commitment was a significant one.

IV. Information matching

INTRODUCTION

Nature of information matching and controls

Information matching, often referred to as data matching, usually involves the computerised comparison of two or more sets of records with the objective of seeking out any records which relate to the same individual in order to detect cases of interest. The process has been referred to as a type of "mass dataveillance" having negative effects upon personal privacy by:

- using information which has been obtained for one purpose for an unrelated purpose;
- "fishing" into government records concerning innocent citizens with the hope of finding some wrongdoing;
- taking automated decisions affecting individuals without human intervention;
- multiplying the effects on individuals of errors in some government databases.

Nonetheless, the technique is believed by many government administrators to have the potential to identify fraud in government programmes. For these, and other reasons, Part X of the Privacy Act, together with the applicable information matching provisions, authorise and regulate the practice of information matching. They do this through controls directed at:

- *authorisation* - ensuring that only matches which appear to be well justified in the public interest go ahead;

- *operation* - ensuring that matches are operated consistently with fair information practices and, given the nature of the technique, that individuals are not "presumed guilty until they prove their innocence";
- *evaluation* - subjecting matches to periodic review so that discontinuance can be considered, unless it can be demonstrated that there are continuing benefits and that matching can be operated consistently with fair information practices.

Section 105 of the Act requires me to report annually in relation to each authorised programme carried out during the year. My 1993/94 annual report was the first in which I did so. Three information matching programmes which had been authorised by earlier legislation had commenced during that year. The number of authorised information matching programmes has continued to grow since then. In this year's report there is material in relation to 11 operational matches. Several more are expected shortly. With so many matches now being reported I have included a small summary table with each match to direct readers to certain basic features of the match including:

- the information matching provision;
- the year authorised;
- the year the match commenced;
- whether the match utilises unique identifiers; and
- whether the match involves the disclosure of information through the use of on-line computer connections.

This year I have included a classification based upon one developed by Dr Roger Clarke of the Australian National University. The eight primary purposes for information matching used in this categorisation are:

- **detection of errors** in programme administration (eg. erroneous assessment of benefit amounts, multiple invoicing);
- **confirmation of continuing eligibility** for a benefit programme, or compliance with a requirement of a programme;
- **detection of illegal behaviour** by taxpayers, benefit recipients, government employees, etc (eg. fraudulent or multiple claims, unreported income or assets, impersonation, omissions, unauthorised use, improper conduct, conflict of interest);
- **monitoring of grants** and contract award processes;
- **location of persons** with a debt to a government agency;
- **identification of those eligible for a benefit** but not currently claiming;
- **data quality audit**;

- **updating of data** in one set of records based on data in another set.

The classification is not used in the Act and is not significant in terms of the requirements of Part X. However, it enables me to offer a useful set of comparisons of the objectives of current matches. It will be seen from the report that a number of matches have more than one purpose under this classification. The present authorised information matching programmes have the following purposes:

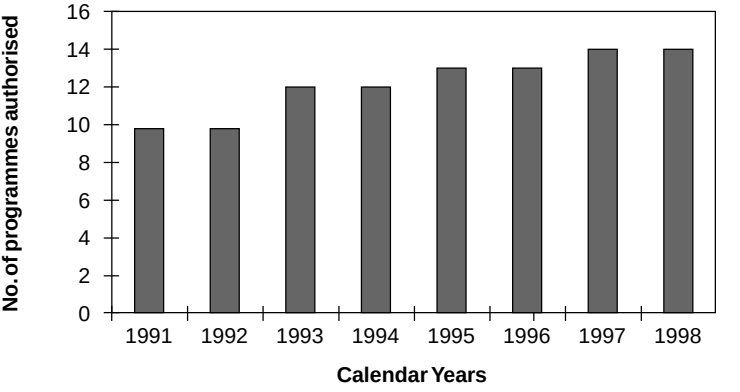
- confirmation of eligibility or continuing eligibility – 8 programmes;
- detection of illegal behaviour – 6 programmes;
- detection of errors – 5 programmes;
- location of persons – 2 programmes;
- updating of data – 1 programme;
- identification of those eligible for a benefit not currently claiming – 1 programme.

Growth in information matching in New Zealand

The Privacy Commissioner Act 1991 created a set of information matching controls and listed the statutory provisions establishing each authorised programme in a schedule. In 1993 the list of information matching provisions was carried over into the Third Schedule of the Privacy Act.

It is now seven years since the first information matching programmes were specifically authorised by statute in 1991. Figure 6 shows the growth in the number of authorised information matching provisions to the

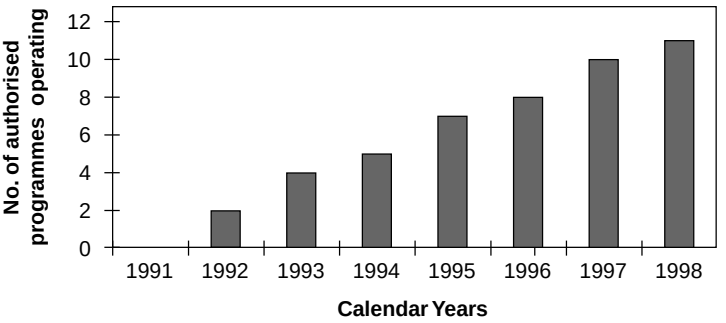
FIGURE 6: INFORMATION MATCHING PROGRAMMES AUTHORISED 1991-1998



present day. The graph masks the amount of legislative activity in relation to information matching since there have been several information matching provisions repealed and others amended or consolidated. Since 1995 there has been a build-up in work for my office in assessing new information matching proposals against the Act's information matching guidelines. Several new programmes remained under consideration at the end of the year.

The growth in the number of information matching provisions enacted does not convey the full scale of the increased information matching activity. A number of information matching provisions enacted in 1991 lay dormant for several years and have only recently begun operation. Figure 7 shows the number of authorised matching programmes operating in each of the years from 1991 onwards. There has been a steady increase in activity with a doubling of the programmes in operation since 1994. This increase has stretched the resources available in my office for carrying out the full monitoring activities contemplated by the Act. This has been compounded in recent years with further work on assessing new information matching programmes, commencing the review of existing provisions under section 106, and the investigation of new information matching complaints.

FIGURE 7: AUTHORISED INFORMATION MATCHING PROGRAMMES OPERATING 1991-1998



Reports to the Minister of Justice during the year

In addition to this annual report on all the programmes carried out during the year, I report to the Minister from time to time on specific matters concerning particular programmes or proposed programmes. During the year I made one report concerning a provision for a new programme and another on an amendment to an existing provision authorising a programme. I also reported to the Minister of Justice in

relation to a matter of particular concern touching upon the operation of the Electoral Match.

Amendment affecting the NZISS/Courts Address Match

The Summary Proceedings Amendment Bill (No 3) proposed to amend section 126A of the Social Security Act, which is the information matching provision authorising the programme between the Department for Courts and the New Zealand Income Support Service (NZISS) to find current addresses of fines defaulters. The existing authorisation allows NZISS to disclose addresses of certain beneficiaries to the Department for Courts. The amendment would allow the additional disclosure of the telephone numbers of those beneficiaries.

Having examined the proposed amendment with reference to the six information matching guidelines set out in section 98 of the Act, I concluded that accuracy of the information was the only significant matter of concern. The departmental assessment was that only 40% of the telephone numbers held were correct. It seemed inappropriate in principle to use information which had been obtained for one purpose for a different purpose after it had been allowed to become inaccurate and out of date, especially where it was to be put to use by the State in the serious task of seeking to enforce court imposed penalties.

Nonetheless, I did not see the data quality problem as being an absolute bar to the amendment proceeding. If the data could be brought up to a good reliable standard my concerns would disappear. Improving the quality of the data would have the added benefit of enhancing the cost-effectiveness of the match. The departments involved indicated that they had plans for improving data quality and I recommended that:

- a methodology be established to verify the accuracy of existing information held, with the results to act as a benchmark;
- NZISS take steps, prior to disclosing any telephone number information to the Department for Courts, to make the information more reliable; and
- the accuracy of the information be measured after such steps have been taken to establish whether improvements have been achieved and whether the information is generally "accurate and up to date".

The bill was reported back from the select committee near the end of the year. The departments convinced the committee that the database had been made more accurate since my report had been written. The amendment was enacted shortly after the end of the year.

New authorised information matching programme – IRD/ Courts

As well as amending section 126A Social Security Act, the Summary

Proceedings Amendment Bill (No 3) introduced a new information matching provision. The new provision would authorise IRD, following a new match, to disclose address and telephone number information to the Department for Courts for use in locating the whereabouts of a taxpayer who is in default in the payment of a fine.

The Department for Courts produced an information matching privacy impact assessment (IMPIA) which described the proposal, the Department's justification for the programme and its views as to compliance with the Privacy Act. The IMPIA contained information about a pilot match the Department had undertaken in order to assist in the calculation of the likely benefits. The Department projected a net annual benefit of $1,284,129 based upon the estimated strike rate calculated from the pilot match and other data.

I examined the proposed provision with reference to the six information matching guidelines. I concluded that the programme related to a matter of significant public importance and would be likely to result in monetary savings which were both significant and quantifiable. I was satisfied that the match could be operated in conformity with the information privacy principles and information matching rules and that the programme was not excessive in scale. Although I had insufficient information from the Department as to alternatives to the programme to assess whether the objectives could be achieved in other ways, the Department and select committee studying the bill were satisfied on that point.

The bill had been reported from the select committee at the end of the financial year and was expected to be passed shortly.

Inaccuracy of list of overstayers - Electoral Match

I submitted a special report to the Minister of Justice in January 1998 expressing concerns about the inaccuracy of source data being used in the Electoral Match.

In 1995, before the Electoral Match was initially authorised, I examined the proposal and reported to the Minister of Justice. I had misgivings as to the data quality of the list of overstayers maintained by the NZ Immigration Service and queried the matter with the Department of Justice. The Department of Justice advised me that the Immigration Service was satisfied its information on persons in New Zealand unlawfully or on temporary permits was "reasonably satisfactory". I indicated in my report that this was not as reassuring as I would like and that I expected the departments to undertake checks on the quality of data for the new purpose before undertaking full scale matching. Inaccurate data might lead to the mismatching of people with the same names and cause distress and humiliation to individuals required to justify their enrolments.

The Auditor-General had undertaken an audit of the Immigration Service in 1994 and made a number of recommendations to improve the existing inaccuracy of the list of overstayers. In 1997 the Auditor-General reported the results of a follow-up audit of the actions taken by the Immigration Service to improve the accuracy of the overstayer list. He concluded that the overstayer list remained "very inaccurate" and had not improved since the 1994 audit.

My 1998 report to the Minister expressed my concern at the inaccuracy of the source data used for this match and recommended temporary suspension of the match pending improvement in data quality. Since the match is only carried out annually, I did not consider that a temporary suspension would be especially problematic for the continued operation of this match. Given the fundamental importance of the right to vote in a democracy, I considered that caution must be exercised before allowing unreliable data to provide the basis for the commencement of a process for disqualifying an elector. If this is at the possible cost of allowing a few names to remain on the roll who are unqualified for residential purposes this must, in my view, be part of the price to be paid until the data can be made reliable.

I was disappointed that the Minister declined to suspend the match, based upon reassurances from officials that sufficient safeguards existed in the challenge processes. Confidence was expressed at the NZ Immigration Service's plans to improve data quality. In my view, notice procedures enabling individuals to justify their enrolment when challenged are no substitute for a match carried out using more accurate data. It is essential that the normal presumption of "innocent until proven guilty" is not allowed to be turned on its head through information matching. Furthermore, the Immigration Service has had a number of years to improve the data quality since the Auditor-General's report of 1994 and to demonstrate such improvement. Reinstatement of the match should follow results rather than promises.

I understand for technical reasons, concerning changes in computer systems, that the information matching programme may not be run for a while. I trust that the departments will use the time to ensure that when matching is resumed it is based upon data of the quality that can be characterised in terms of information privacy principle 8 as "accurate and up to date".

Information matching: activity at the Office of the Privacy Commissioner

In February 1998 changes were made to the Privacy Commissioner's

team handling information matching matters. Blair Stewart, Manager, Codes and Legislation, took on the responsibility for monitoring information matching activity, which was formerly undertaken by Robert Stevens. Prior to this Blair Stewart had overseen the assessment of proposals for new information matching programmes as part of his legislative responsibility. The role was extended to the monitoring of operating programmes and their periodic reassessment. Michael Wilson assisted for two days a week on information matching matters. Robert Stevens continues to be used on an occasional contract basis for some information matching projects.

Within these limited resources it has been difficult to cope with the greatly expanded monitoring workload, together with the assessment of the many new information matching legislative proposals which have surfaced over the last few years. Expansion of matching activity shows no sign of slowing.

One major activity during the year under review has been the review of the operation of the Privacy Act pursuant to section 26. This has included an examination of information matching issues and involved the release of a questionnaire to all agencies participating in information matching early in 1997 and a full public discussion paper on the topic later that year. A number of recommendations bearing upon Part X are expected in the Commissioner's report to be released later in 1998.

One of the results of giving priority to the section 26 review has been a further delay in the review of information matching provisions under section 106. That latter section requires me to review the operation of each information matching provision and to report my findings as soon as practicable after 1 January 1994. I repeatedly deferred plans to conduct the review because I considered that the paucity and unreliability of the figures available in relation to the key programmes rendered the review impracticable. However, having lost faith in promises of early improvement in reporting, I resolved to carry out the review during 1996/97. While a start was made on that review it was not completed in that year or indeed in this. I now intend to undertake the section 106 review in more manageable batches, with the first ones to be completed during the 1998/99 year. My first priority will be in relation to the matches authorised in 1991, which have been operating for several years since 1993. More recently authorised matches will be reviewed in later batches.

As resources permit I would like to devote more attention to initiatives designed to enhance compliance across the board rather than those simply directed at individual matches. Proposals in this regard include workshops for policy advisers and officials involved in information matching, the

development of an information matching manual and publication of further guidance materials. One initiative taken in March 1998 was the first issue of an information matching bulletin intended to disseminate basic information and developments to staff across departments working in the area. Two new compilations of materials on information matching, including all reports to the Minister and annual reports, were also prepared during the year.

Since NZISS is involved in many of the existing matches I will make some general comments about the reports I have received from that department before moving to the match by match discussion.

General comments about NZISS reports

In previous annual reports I have commented unfavourably on the reports received from NZISS for their main information matching programmes. There were numerous matters on which NZISS advised they could not, or simply did not, report to me. Where figures were reported to me I detected a variety of problems which called their reliability into question.

This year some of those problems have been resolved. One factor in the improved reliability of the figures may be the centralisation in late 1996 of NZISS's operation at their Lower Hutt "Datamatch Centre". The Centre is in a position to ensure that NZISS's policies for handling responses from beneficiaries are uniformly applied. Previously, data entry relied upon staff in district offices around the country who did not always follow the same procedures.

However, some problems remain to be resolved with the reports. I am advised by NZISS that solutions to these problems are complex. For example, some of the information about which I have requested reports is not recorded by the computer used for processing information matching results. Any solution would therefore involve changes to the computer programme or NZISS's methods of operation.

My requirements for additional data or checks have languished for several years in the "queue" of demands for changes to the NZISS computer programmes. It appears that other priorities always put data matching computer modifications back.

An attempt to get around the problem this year by the Datamatch Centre involved the purchase of a "front-end" search programme which was installed onto the database run by NZISS to retrieve otherwise uncollated statistics. This programme was only partly successful, although NZISS have reported a growing confidence in reports being produced.

In a general report to me this year, NZISS included details of system enhancements for the Datamatch Centre database. These include safeguards to ensure the requirements of section 101 cannot be overrun in error, preventive measures to ensure that updating records can only take place within the permitted periods and other security measures. These enhancements appear to be amongst a number of initiatives which are designed to improve the reliability of reports received in 1998/99.

Recoveries

The reliable reporting of recoveries has been a major deficiency in previous years' reports. Recoveries of money, as opposed to debts being "established", are carried out by the five Regional Debt Collection Units at NZISS. The National Debt Management Unit, which is responsible for analysing debt recovery results from the Regional Units, has been unable to re-code established debt data already held by NZISS to allow the tracing of "datamatch" debt to determine whether, and in what amounts, it is actually recovered by NZISS. Because "datamatch" debt could not be separated from debt established by other means, the actual recoveries obtained by NZISS from information matching could not be ascertained with any assurance of accuracy.

To counter this, the National Debt Management Unit commenced a new procedure from July 1997 which entailed encoding new data entered on the SWIFTT database with a certain code. After one year, debt established since July 1997 should be traceable while the debtor is currently receiving a benefit, to determine whether the information matching debts are actually paid. This innovation is a laudable (if overdue) attempt to overcome one of the major problems to date with NZISS reporting of information matching results.

However, SWIFTT data relates only to debts established against those individuals currently receiving a benefit. As yet, "datamatch" debtors who are not currently receiving a benefit, and thus recorded on a different database (TRACE), cannot be tracked because, again, the data match derived debt is not separated from the debt derived from other sources. Nonetheless, NZISS has produced a series of estimates of debt recovered for TRACE debtors. These estimates are an improvement in reliability on previous years because the amount of debt transferred from SWIFTT to TRACE can be tracked to the point of transfer due to the new encoding system in SWIFTT. From there, NZISS have estimated the amounts recovered.

The results of the SWIFTT and TRACE estimated recoveries and totals are set out below. The SWIFTT recoveries include estimates of recoveries from debts established before the new coding system was commenced.

TABLE 10: NZISS ESTIMATE OF ACTUAL RECOVERIES 1997/98

Month	SWIFTT Recoveries (part estimated and part measured)	Trace Recoveries (estimated)	Total Recoveries
July-97	$226,459	$474,092	$700,551
August	$207,655	$509,463	$717,118
September	$260,358	$454,468	$714,826
October	$217,046	$500,597	$717,643
November	$236,852	$446,389	$683,241
December	$222,639	$470,450	$693,089
January-98	$212,802	$404,722	$617,524
February	$227,013	$430,805	$657,818
March	$290,008	$477,440	$767,448
April	$231,535	$474,153	$705,688
May	$233,783	$470,940	$704,723
June	$266,272	$513,916	$780,188
TOTAL	$2,832,422	$5,627,435	$8,459,857

The amounts recovered seem to be substantially less than the amounts reported to me in previous years as recovered (see table 11). In previous annual reports I have noted at some length that the estimates of recovery were disappointingly inaccurate, derived as they were from various estimates and guesses. The estimates for this year seem to be more reliable since they are derived in part from some actual data recorded by the SWIFTT database. While the amount of debt established has not decreased, decreases in the level of reported recoveries may well indicate a more realistic level of reporting rather than any material changes in the actual amounts recovered. Overseas experience suggests that the amounts recovered from data matching are often considerably less than expected, and therefore previous years' estimates may have erred on the side of optimism. It is difficult to see how NZISS will now be able to produce retrospectively any reliable figures for those previous years.

Costs

The summary of costs provided to me this year was more detailed than in previous years. NZISS broke the costs down into several separate headings, including the cost of notices of adverse action, staff time, general expenses, overheads, and information technology costs. The

figures were further broken down into monthly expenditure figures.

I have expressed dissatisfaction in the past about NZISS's failure to break down the costs of these information matching programmes into separate totals for the various programmes, that is, Customs, Corrections, Inland Revenue and Education. Centralisation has had some advantages in respect of the information obtained from NZISS in other areas, but as yet I am unaware of any positive effect in the area of breaking down costs by matching programme.

Results

Set out below are the overall results for the combined totals of the four main NZISS information matching programmes, namely:

- Customs/NZISS;
- Corrections/NZISS;
- Education/NZISS, and
- IRD/NZISS Commencement/Cessation.

TABLE 11: COMBINED TOTALS OF THE FOUR MAIN NZISS PROGRAMMES

Recoveries	**1995-96**	**1996-97**	**1997-98**
Overpayments established – number	38,093	26,242	33,568
Overpayments established – amount	$28,862,276	$20,653,380	$30,372,465
Penalties imposed – number	11,548	5,161	28
Penalties imposed – amount	$9,983,951	$4,904,918	$16,938
Total debts established – amount	$38,846,227	$25,558,298	$30,389,403
Prospective savings – number	3,934	1,424	(1)
Prospective savings – amount	$10,145,554	$3,521,818	(1)
Recoveries	$15,708,733(2)	$16,450,678(2)	$8,459,857(3)
Cost of operations	$13,200,510	$9,855,461	$8,215,897(4)

(1) no longer calculated
(2) estimated
(3) estimated, using new method of calculation
(4) made up of Datamatch Centre costs added to Debt Recovery Unit costs

PROGRAMME BY PROGRAMME REPORTS

Introduction

The following material reports on each of the authorised information matching programmes in operation and two which have been authorised but are not yet fully operational. A report is also included for the programme carried out under section 11A of the Social Security Act. Although that section is not an information matching provision, I am required to report on the matches carried out under that section as if it were.

For the purposes of this report I have given each match a title. Each title commences with the names of the agencies involved and in some cases this is followed with a description. I have adopted the convention of first naming the agency whose only role is as a source of information to be matched. The agency making use of the discrepancies produced by the match is named second. For example, in the "NZISS/Courts Address Match" the role of NZISS is to supply the information to be matched with data from the Department for Courts but it does not use the results to take action against any individual. The Department for Courts uses the discrepancies for its purposes. In this case, the programme is an "address match" which means that addresses are disclosed to the Department for Courts to enable matched individuals to be traced.

Each entry commences with a table setting out basic information about the match. A description of the purposes of the match and how it is carried out follows. In the balance of each entry there is discussion of notable issues arising from the operation of the match during the year, a table of results and some brief commentary on those results.

The reports are set out in the following order:

Matches with NZISS as user agency

- Corrections/NZISS match
- Customs/NZISS match
- Education/NZISS match
- IRD/NZISS Commencement/Cessation match
- NZES/NZISS match
- IRD/NZISS Address match
- Section 11A Social Security Act match
- IRD/NZISS Community Services Card match

Matches with other departments as user agency

- NZISS/Courts Address match
- NZISS/IRD Child Support match

- NZ Immigration Service/Electoral Enrolment Centre match
- IRD/ACC match

CORRECTIONS/NZISS MATCH

Information matching provision	Penal Institutions Act 1954, s.36F
Year authorised	1991
Commencement date	April 1995
Match type	• Detection of errors • Confirmation of continuing eligibility • Detection of illegal behaviour
Unique Identifiers	None
On-line transfers	None

The Corrections/NZISS Match is designed to detect beneficiaries receiving Income Support who are imprisoned and are therefore ineligible for benefits. The programme operates by a weekly transfer of information about all newly admitted inmates from the Department of Corrections to NZISS.

The information is compared by name and date of birth. Comparison had also been made in previous years by gender but that proved unreliable because of different gender coding practices between the departments. Matched individuals are sent a notice advising them that, unless they produce proof to the contrary, the benefits which they are receiving from NZISS will cease and any overpayment found to have been made will be established as a debt to be repaid to NZISS.

Results

TABLE 12: CORRECTIONS/NZISS MATCH 1997/98

Corrections/NZISS Match As at 30/6/98 TOTAL: 1997/98	
number of runs	50 (for 1997/8)
number of records compared	not available
number of "positive" matches	11,157
legitimate records (no adverse action taken)	4,296
notices of adverse action issued	8,662
mismatches	43
debts established	2,917
overpayments established	$1,791,806
challenges	3
unresolved at 30/6/98	2,253

These figures represent returns to 30 June 1998 on matching runs carried out in 1997/98. The Datamatch Centre also processed some results from runs carried out in 1996/97 but for which processing was not complete until this financial year. If the last quarter of this year is extracted from the above figures and the last quarter of the previous year is inserted, for which processing is now complete, a better "snapshot" of the scale of the programme emerges.

TABLE 13: CORRECTIONS/NZISS MATCH: LAST QUARTER 1996/97 – END THIRD QUARTER 1997/98

Corrections/NZISS Match As at 30/6/98 TOTAL: Last quarter 1996/97 to end of Third Quarter 1997/98	
number of runs	50
number of records compared	not available
number of "positive" matches	11,231
legitimate records (no adverse action taken)	4,359
notices of adverse action issued	6,872
mismatches	44
debts established	3,713
overpayments established	$2,168,973
challenges	3
unresolved at 30/6/98	1,316

The biggest difference between results in tables 12 and 13 is in the amount of debt established (considerably higher in the second table) and in the number of unresolved cases (considerably lower in the second table, including 317 cases from the last quarter of 1996/97, for which the time limits in section 101 may have expired). These differences are due to the fact that more runs have been completely processed in the second table.

On the basis of the information supplied, I am satisfied that this programme has been conducted in accordance with the requirements of sections 99 to 103 of the Privacy Act and the information matching rules. This is subject to my general comments about reports made by NZISS.

CUSTOMS/NZISS MATCH

Information matching provision	Customs and Excise Act 1996, s.280
Year authorised	1991
Commencement date	June 1992
Match type	• Confirmation of continuing eligibility • Detection of illegal behaviour
Unique Identifiers	None
On-line transfers	None

The Customs/NZISS Match is designed to detect those who travel overseas while receiving a benefit. Some benefits, such as unemployment, may not be paid at all when the individual is overseas. Others, such as superannuation, may be paid for only a specified period while the individual is overseas. This period varies from benefit to benefit.

The programme operates by a transfer of arrival and departure information once a week from NZ Customs Service (Customs) to NZISS of those arriving in and departing from New Zealand. The information is compared with NZISS's database of beneficiaries by name, date of birth, and gender. The information provided to NZISS also includes passport number, flight number, country of citizenship, and dates of arrival or departure.

NZISS then check their records to determine whether there is an explanation known to NZISS for the journey overseas. If there is no explanation, the matched individual is sent a notice advising that, unless they produce proof to the contrary, the NZISS benefit may cease and any overpayment will be recovered from the individual. Where a benefit may be paid for a certain period while the individual is overseas, NZISS does not issue a notice of adverse action until the requisite period passes and the individual remains out of New Zealand.

Section 103(1A)

The Customs/NZISS programme has a unique feature. Subsection 103(1A) permits NZISS to suspend *immediately* a person's benefit if a discrepancy arises pursuant to the Customs/NZISS information matching programme, provided a notice of adverse action is issued before or immediately after the decision has been made to suspend the benefit. This contrasts with the normal operation of section 103 whereby no "adverse action" (such as stopping a benefit payment) may be taken until 5 days after a notice of adverse action has been delivered.

In introducing subsection 103(1A) in mid-1993 the Government relied upon advice from NZISS that the programme would be unworkable

without this dispensation. However the provision has never been used by NZISS and yet the programme is regarded by its users as one of the more efficient and effective matches. I opposed the enactment of section 103(1A) and remain of the view that it should be repealed.

Publicity

Rule 1 of the information matching rules provides that the individuals who will be affected by the information matching programme should be advised of it by the agencies involved taking all reasonable steps to notify them of the programme. These steps "may consist of or include public notification".

Recently NZISS updated its information leaflets describing the various benefits. Under the heading "Departure overseas" the new leaflets referred, in passing, to the information matching programme with Customs as a programme which "may" mean that departures overseas will be monitored. I consider that this point should be made more clearly in the leaflets and any other publicity materials, such as by saying that departures overseas "will" be monitored by the programmes. It is possible that such statements may deter individuals from attempting to continue to receive income while overseas if they know they "will" be monitored. I have recommended that NZISS reconsider the wording on this point in the next update of their leaflets.

Notice in cases where the individual may be out of New Zealand for a certain period before becoming ineligible for a benefit

NZISS does not issue notices of adverse action to those who depart New Zealand who receive a benefit which is stopped only when the person has been out of the country for a certain period and has not returned within that period. In the case of superannuation, for example, the recipient is permitted to be absent from New Zealand for six months before the absence affects the entitlement to superannuation payments. If the recipient is out of New Zealand for more than 30 weeks, the entire benefit paid from the time the individual left the country must be repaid by the individual. Thus when overpayments occur in the case of superannuation payments, they will always be substantial. The department may possibly diminish these overpayments by notifying superannuitants that, unless they return to New Zealand before a certain date, they may forfeit some or all of their superannuation. I expect that people going abroad for extended periods would frequently arrange for their mail to be forwarded or monitored.

Results

These figures represent returns to 30 June 1998 on matching runs carried out in 1997/98. The Datamatch Centre also processed some results

TABLE 14: CUSTOMS/NZISS MATCH 1997/98

Customs/NZISS Match As at 30/6/98 TOTAL 1997/98	
number of runs	52
number of records received from Customs	3,919,190
number of "positive" matches	23,888
legitimate records (no adverse action taken)	5,474
notices of adverse action forwarded	13,539
mismatches	35
debts established	10,429
overpayments established	$5,240,816
challenges	9
unresolved at 30/6/98	5,099

TABLE 15: CUSTOMS/NZISS MATCH: LAST QUARTER 1996/97 - END THIRD QUARTER 1997/98

Customs/NZISS Match As at 30/6/98 TOTAL: Last quarter 1996/97 to end of Third Quarter 1997/98	
number of runs	52
number of records received from Customs	3,993,281
number of "positive" matches	22,994
legitimate records (no adverse action taken)	5,275
notices of adverse action forwarded	17,719
mismatches	55
debts established	11,478
overpayments established	$6,155,581
challenges	10
unresolved at 30/6/98	2,711

from runs carried out in 1996/97 for which processing was not complete until this financial year. If the last quarter of this year is extracted from the above figures and the last quarter of last year is inserted, for which processing is now complete, a better "snapshot" of the scale of the programme emerges.

The biggest difference between these two sets of results is in the amount of debt established (considerably higher in table 15) and in the number of unresolved cases (considerably lower in table 15). These differences are due to the fact that more runs have been completely processed in table 15.

On the basis of the information supplied, I am satisfied that this programme has been conducted in accordance with the requirements of sections 99 to 103 and the information matching rules. This is subject to my general comments about reports made by NZISS.

EDUCATION/NZISS MATCH

Information matching provision	Education Act 1989, s.307A
Year authorised	1991
Commencement date	October 1992
Match type	• Detection of errors • Confirmation of continuing eligibility • Detection of illegal behaviour
Unique Identifiers	Tax file number
On-line transfers	None

The Education/NZISS Match is designed to detect those on the unemployment or sickness benefits who are also receiving a student allowance or studying full-time. The programme is designed to prevent "double-dipping". It is carried out three times a year.

The programme operates by NZISS forwarding a diskette with the names of those receiving the relevant benefits to the Ministry of Education. The student allowance database held by the Ministry is compared with that of NZISS, using the tax file number as the only basis for a match. Any matches are then returned to NZISS by the Ministry of Education.

NZISS checks the enrolment status of matched individuals with the relevant tertiary institution. Individuals for whom full-time enrolment is confirmed are sent a notice advising them that, unless they produce proof to the contrary, the benefit they are receiving from NZISS will cease and any overpayment found to have been made will be established as a debt to be repaid to NZISS.

The programme operates much as it did in 1992 when it was first instituted. I understand that the programme will cease to be an authorised information matching programme when the new department (to be known as Work and Income New Zealand) combines the roles of New Zealand

Employment Service and NZISS and takes over the payment of student allowances. This means that the Education Match as it has been to date will no longer take place.

Matching criteria

The Education Match has operated by comparing information on each department's database by using the tax file number (TFN) to find similarities. NZISS have indicated that this has caused difficulties because many students do not record their TFN properly. Many students would no doubt be using such numbers for the first time. Thus, the match produces relatively few discrepancies and is known by the Department to be inefficient (a point I return to below in the summary of some of the results of this programme).

When questioned why the TFN alone was used, in a match in which the Inland Revenue Department is not involved, NZISS has always replied that the legislation does not provide for any other matching criteria to be used. However the authorising section (section 307A of the Education Act 1989) does *not* prevent other criteria being used. The section states that the information which may be exchanged may *include* the TFN, which simply authorises the use of the TFN in a match in which Inland Revenue is not involved. It does not limit the possible matching criteria to the TFN.

Using the TFN as an identifier for a matching programme to which Inland Revenue is not a party is a practice which I discourage. The experience of this programme amply demonstrates its practical difficulties.

Summary of a selection of results

In the following two tables, I have set out the results of the information matching programme as reported to me for two runs of the Education/NZISS match. The 12 month time limit prescribed in section 101(2) of the Privacy Act has expired for both of these matching runs, so the figures are "complete". These are the latest "13 month", or completed, reports I have received.

I have referred above to NZISS's comments concerning the efficiency of this match. These tables of results appear to bear out NZISS's concerns.

For example, in the results recorded for the run dated 15 December 1996, 202,396 records were compared. Only 118 positive matches were found. Of these, 41 were "legitimate", that is, an explanation was found on NZISS's records which meant that no adverse action would be taken. Six of the remainder were not proceeded with due to expiry of the time limit in section 101(2).

The Datamatch Centre has indicated to me the belief that a large (but unmeasured) number of potential matches are not detected because the TFN is wrongly recorded by the student when registering with the Ministry of Education. There is no evidence to determine whether these

are mostly either deliberate or innocent errors. However, in view of this, NZISS have indicated they consider the programme would run considerably more efficiently if matching was by name or other criteria in addition to the TFN.

As this match will be discontinued in the near future, at least in its present form, there is no continuing need to address these issues. However, the expected issue late in 1998 of "IRD Information Cards" to student loan borrowers and youths between 15 and 18 who have a TFN is a belated attempt to tackle the problem.

TABLE 16: EDUCATION/NZISS MATCH – 13 MONTH REPORT FOR RUN DATED 30/9/96

Education /NZISS Match 13 month report (30/09/97) for run dated 30/9/96	
Number of records compared	197,587
Number of "positive" matches	163
Legitimate records (no adverse action taken)	9
Notices of adverse action issued	154
Mismatches	2
Debts established (number)	92
Debts established (amount)	$205,312
Challenges	0
Unresolved at 13 month date (not proceeded with)	3

TABLE 17: EDUCATION/NZISS MATCH - 13 MONTH REPORT FOR RUN DATED 15/12/96

Education/NZISS Match 13 month report (15/12/97) for run dated 15/12/96	
Number of records compared	202,396
Number of "positive" matches	118
Legitimate records (no adverse action taken)	41
Notices of adverse action issued	77
Mismatches	0
Debts established (number)	62
Debts established (amount)	$143,945
Challenges	0
Unresolved at 13 month date (not proceeded with)	6

Documentation of changes to the programme

NZISS has made a number of changes to the Education Match over the last few years without updating the documentation supporting the programme, namely the information matching agreement and the Technical Standards Report. One change saw the programme expanded to include institutions in addition to the seven universities.

An information matching agreement defines the terms of the arrangement between the parties to the information matching programme, in this case NZISS and the Ministry of Education. It is required by section 99 of the Privacy Act. Section 99(4) requires the agreement and any variations to it to be forwarded to me "forthwith". The Technical Standards Report, required by information matching rule 4, sets out the way in which the programme operates. Rule 4(5) requires the Technical Standards Report and any amendment to be forwarded to me. By this means, I am supposed to be kept informed as to developments in the information matching programmes. That did not happen in this case. In these respects, it is apparent that the programme has not complied with all of the obligations in sections 99 to 103 and the information matching rules of the Privacy Act.

Complaints

I received two complaints about the operation of this matching programme during the course of this year. They remain under investigation.

IRD/NZISS COMMENCEMENT/CESSATION MATCH

Information matching provision	Tax Administration Act 1994, s.82
Year authorised	1991
Commencement date	March 1993
Match type	• Detection of errors • Confirmation of continuing eligibility • Detection of illegal behaviour
Unique Identifiers	Tax file number
On-line transfers	None

The IRD/NZISS Commencement/Cessation Match is designed to detect those who are receiving a benefit and working at the same time. The programme operates by an exchange of information six times a year between the Inland Revenue Department (IRD) and NZISS. NZISS provides the names of individuals receiving income support to IRD to compare with those people recorded on its database. Where a match is found, the matched individual's details of income and the periods of income are passed to NZISS. Any matched individuals are then investigated further by NZISS to determine whether the individual has earned amounts over

the limit set for the relevant benefit. A check of the records held by NZISS is done to determine whether there is already an explanation for the match on NZISS's records. If there is no explanation, the matched individual is sent a notice advising that, unless they produce proof to the contrary, the presumed employer will be contacted to confirm dates of employment and amounts earned. If the employer confirms these matters, then the NZISS benefit may cease, and any calculated overpayment will be established as a debt to be recovered from the individual.

The individuals whose names are submitted to the matching programme are chosen by one of three ways:

- all those individuals who commence or cease receiving a benefit in the period since the last match;
- any Area Benefit Crime unit may nominate specific individuals whom they are investigating;
- one sixth of all those enrolled with NZISS.

This last group will be a different sixth of those enrolled for each match per year, so that in the course of 12 months all those enrolled with NZISS will have had their records matched with IRD at least once.

Summary of a selection of results

In the following tables, I have set out the results of the information matching programme as reported to me for five matching runs of the IRD/NZISS Commencement-Cessation match. The twelve month time limit prescribed in section 101(2) of the Privacy Act has expired for all of these matching runs, so the figures are "complete". I have been advised that Runs 21 and 23 were abandoned because of difficulties in completing the processing of the runs at the time of the centralisation of the Datamatch Centre.

TABLE 18: IRD/NZISS COMMENCEMENT/CESSATION MATCH 13 MONTH REPORT FOR RUN 20

IRD/NZISS Commencement/Cessation Match 13 month report (3/11/97) for run 20 dated 3/10/96	
number of records compared	102,334
number of "positive" matches	24,504
legitimate records (no adverse action taken)	17,090
notices of adverse action forwarded	7,414
mismatches	5
debts established (number)	1,347
debts established (amount)	$1,211,830
challenges	102
unresolved at 13 month date (not proceeded with)	667

TABLE 19: IRD/NZISS COMMENCEMENT/CESSATION MATCH 13 MONTH REPORT FOR RUN 22

IRD/NZISS Commencement/Cessation Match 13 month report (15/2/98) for run 22 dated 15/1/97	
number of records compared	168,937
number of “positive” matches	41,568
legitimate records (no adverse action taken)	27,296
notices of adverse action forwarded	14,272
mismatches	1
debts established (number)	2,189
debts established (amount)	$2,330,920
challenges	190
unresolved at 13 month date (not proceeded with)	1,074

TABLE 20: IRD/COMMENCEMENT/CESSATION MATCH 13 MONTH REPORT FOR RUN 23

IRD/NZISS Commencement/Cessation Match 13 month report (22/4/98) for run 23 dated 22/3/97 Run abandoned before full investigation	
number of records compared	125,018
number of “positive” matches	30,407
legitimate records (no adverse action taken)	30,113
notices of adverse action forwarded	294
mismatches	0
debts established (number)	13
debts established (amount)	$7,710
challenges	0
unresolved at 13 month date (not proceeded with)	53

TABLE 21: IRD/NZISS COMMENCEMENT/CESSATION MATCH 13 MONTH REPORT FOR RUN 24

IRD/NZISS Commencement/Cessation Match 13 month report (14/6/98) for run 24 dated 14/5/97	
number of records compared	112,160
number of "positive" matches	28,647
legitimate records (no adverse action taken)	18,684
notices of adverse action forwarded	9,963
mismatches	1
debts established (number)	2,887
debts established (amount)	$3,081,342
challenges	110
unresolved at 13 month date (not proceeded with)	2,355

On the basis of the information supplied, I am satisfied that this programme has been conducted in accordance with the requirements of sections 99 to 103 of the Privacy Act and the information matching rules. This is subject to my general comments about reports made by NZISS.

NZES/NZISS MATCH

Information matching provision	Social Security Act 1964, s.131A
Year authorised	1997
Commencement date	1997
Match type	• Confirmation of continuing eligibility • Updating of data
Unique Identifiers	SWIFTT (NZISS) number and NZES number
On-line transfers	Approvals granted (25 June 1996, 31 March 1998 and 1 May 1998)

The information exchange between NZ Employment Service (NZES) and NZISS takes place several times a day and is designed to allow each department to keep up-to-date records of those registered with both departments. The records include whether the individual had received a work-tested benefit, whether the individual had failed a worktest, lapse of an individual's enrolment with NZES, and so forth. The information flows in both directions.

Information exchange is by means of an on-line computer connection,

for which approval was granted by the Privacy Commissioner under information matching rule 3. The most recent approval was given on 1 March 1998 and continues until 1 October 1998.

Discontinuance of programme

This information matching programme will, by the time of publication of this report, have been discontinued as an authorised information matching programme because of the amalgamation of NZES and NZISS into one department, Work and Income New Zealand (WINZ). The exchange of information between these two component parts of a single department will, in this case, be of a different character from the present matching between two separate government agencies. Section 131A of the Social Security Act will be repealed by the Employment Services and Income Support (Integrated Administration) Bill before 1 October 1998. I understand that, for the time being, the computer systems remain separate so the information will continue to be communicated by the same procedures. However, the process will not involve separate departments and will no longer be carried out pursuant to an authorised information matching provision.

On-line Transfer

This information matching programme was the only one operated with an on-line transfer approval granted pursuant to information matching rule 3. The first approval was granted on 25 June 1996, a renewal was granted on 31 March 1998, and a further renewal to 1 October 1998 was issued on 1 May 1998.

One of the conditions of the original approval granted was that an internal audit be conducted of the transfer of information to check compliance with the approval. Audit reports from each department were forwarded to me. The auditors generally concluded that there had been compliance with the requirements of the on-line transfer approval. However, the audit reports contained some comments by the auditors about certain compliance and data security issues. Recommendations were made by the auditors to address these matters.

Reporting difficulties

In March 1998, NZISS wrote to me indicating that there were problems with the Department's ability to report in terms of section 104 of the Privacy Act. Discussions had been ongoing on such issues for some time. NZISS indicated to me that it would be required to spend a substantial sum to institute a computer program to capture the information on which I had asked them to report. As it became clear that the two departments would merge, and the match would be discontinued, I concluded that it was undesirable to spend such a sum to correct the

deficiencies.

Consequently, I received only minimal reports from NZISS in relation to this matching programme. Some issues were canvassed fully, such as compliance with Rule 6(2) and the on-line transfer audit report. Other issues such as how many notices of adverse action had been issued for the entire year and how many challenges there had been, and some other matters calculating the scope of the programme, were not reported on fully. As a consequence I cannot indicate that there has been compliance by NZISS in respect of the main issues under Part X of the Privacy Act or the information matching rules.

Some of the results forwarded to me in March 1998 included the results contained in the two tables opposite.

The notices of adverse action issued by NZISS were the subject of several complaints this year. Section 131C of the Social Security Act provides that the notice must set out certain matters, including giving individuals 5 working days' notice of any change to their benefit payments due to failure of the work test. My investigation is continuing.

IRD/NZISS ADDRESS MATCH

Information matching provision	Tax Administration Act 1994, s.85
Year authorised	1993
Commencement date	November 1994
Match type	Location of individuals
Unique Identifiers	Tax file number
On-line transfers	None

The IRD/NZISS Address Match is designed to provide NZISS with up to date addresses from IRD for those who owe money to NZISS. These debts arise due to benefit overpayments having been established. The debtors traced through the programme are debtors who are not currently receiving a benefit and for whom NZISS has lost contact. The programme is one part of NZISS's process of collecting debts established by the other NZISS information matching programmes, as well as from other NZISS operations.

Results

A summary of the main results for the last three years is detailed below (table 24).

The figures for numbers of matches which result in adverse action being taken are showing a decline. NZISS has not conducted any studies to determine exactly why this is so, but has suggested that a backlog of

TABLE 22: WORK TEST EVENTS (APRIL 97 - JANUARY 98) RELATING TO WORK TEST FAILURES

Work Test Event Result	Apr	May	June	July	Aug	Sept	Oct	Nov	Dec	Jan'98	Grand Total
Potential Failure	482	576	560	845	925	1047	1360	1424	1086	1190	9495
Pass	174	374	361	509	564	645	835	846	839	718	5865
Recommended Failure	22	51	40	100	92	145	201	216	203	167	1237
Approved Failure	5	28	24	53	50	100	140	165	162	123	850
Failure Not Approved	3	10	12	17	16	34	50	31	17	24	214
Recomplied	1	7	9	37	17	38	75	105	116	104	509
Grand Total	687	1046	1006	1561	1664	2009	2661	2787	2423	2326	18170

TABLE 23: WORK TEST EVENTS (APRIL 97 – JANUARY 98) RELATING TO APPEALS AND CHANGES TO WORK TEST ELIGIBILITY

Work Test Event	Result	Apr	May	June	July	Aug	Sept	Oct	Nov	Dec	Jan'98	Grand Total
Appeal	Upheld	0	1	0	0	0	1	1	0	0	0	3
	Withdrawn	0	0	0	0	1	0	1	0	0	0	2
Work Test Deactivated	In work 10 days	0	0	0	1	1	2	2	0	0	0	6
	Not work testable	31	177	226	298	298	437	350	448	355	507	3127
Work Test Stop	Change to part time	0	0	0	0	0	0	1	0	0	0	1
Grand Total		31	178	226	299	300	440	355	448	355	507	3139

TABLE 24: IRD/NZISS ADDRESS MATCH RESULTS 1996-1998

IRD/NZISS address match	1995/96	1996/97	1997/98
Number of runs	4	6	5
Debtors sent for matching *(A)*	251,410	337,211	256,324
Average number of debtors per run	62,852	56,202	51,625
Matched by IRD *(B)*	198,298	295,801	230,174
% of debtors sent *(B/A)*	78.9%	87.7%	89.8%
Matches found useable *(C)*	68,150	70,339	45,047
% of debtors sent *(C/A)*	27.1%	20.9%	17.6%
% of those matched by IRD *(C/B)*	34.4%	23.8%	19.6%
Letters sent out *(D)*	29,196	18,392	7,708
% of those matched by IRD *(D/B)*	14.7%	6.2%	3.3%
% of matches found useable *(D/C)*	42.8%	26.1%	17.1%
Letters not returned (presumed delivered) *(E)*	23,374	15,336	6,482
% of matches found useable *(E/C)*	34.3%	21.8%	14.4%
% of letters sent out *(E/D)*	80.1%	83.4%	84.1%
Estimated payments received	$1,500,000	$980,847	$657,484
Costs reported by NZISS	$232,219	$222,357	*

* No comparable figure for 1997/98.

old debts was cleared in the first few runs of the matching programme. NZISS also advise that they have instituted more efficient procedures for staying in contact with debtors from the time the debt is established. There are consequently fewer debtors with whom NZISS have lost contact, so there is less need to resort to the Address Match to locate debtors.

Reporting of recoveries of debt

Reports received from the division of NZISS which collects debts have generally been reliable and useful for the address match. However, one problem common to all the NZISS programmes is the difficulty in tracking debt actually recovered as distinct from debt which has been established (quantified and notified to the debtor). The solution to this problem involves a new coding category for coding datamatch-established debt from the time it is first entered on the database. This is further noted under the heading of “NZISS reporting”.

Of the amounts recovered, NZISS have reported the amounts of which they are certain as the "minimum" amounts recovered. The reports for this match are received after the 60 day time limit in section 101 has expired. Thus the figures under the headings labelled A to E in table 24 contain "final" numbers. However, recovery can take some years because some debtors do not commence paying debts for some time, or continue to pay at a slow rate for many years. So the recoveries which are reported relate only to the amounts recovered for the runs carried out in that specific year to the date of the report.

SECTION 11A OF THE SOCIAL SECURITY ACT

Commencement date	1987 (1993, altered to include certain duties under Part X of the Privacy Act)
Category of match type	Detection of illegal behaviour
Unique Identifiers	Not applicable
On-line transfers	Not applicable

Section 11A of the Social Security Act 1964 authorises the Director-General of Social Welfare to request information from employers about their employees or a specified class of employees (including former employees). The information may include names and addresses and tax file numbers. Section 11A(3) prevents the Director-General requesting information from the same employer within a 12 month period. The information thus obtained may then be compared with records of social welfare benefits paid out. Any discrepancies found are dealt with in terms of section 11A. Sections 11A(6) and (7) bring the operation of the information matching programme under Part X of the Privacy Act.

Reports to my office on the operation of this programme were not available last year in time for inclusion in my annual report, but I am pleased that I have now received those 1996/97 reports as well as the reports to June 1998.

The following table contains a summary of the last three years of operation. In this table:

- numbers for "matches" refer to the number of employers approached by NZISS under section 11A.
- section 11 letters seek further information from the employer about a specific employee: the employer may receive numerous letters, one for each employee for whom further information is being sought. The section 11 letter is a further "step" in the section 11A programme.

Results

TABLE 25: OUTCOMES OF SECTION 11A MATCHING OPERATIONS

	1995/96 (completed)	**1996/97 (to 23/02/98)**	**1997/98 (to 20/7/98)**
Matches approved	28	23	119
Matches completed	28	14	42
Matches not completed	0	9	77
Details of completed matches			
Total employees checked	10,184	3,495	7,093
Section 11 letters to employers (one letter per individual employee being investigated)	1345	813	539
Notices of adverse action (issued to employees who appear to have been working while receiving a benefit)	823	439	325
Overpayments detected (number)	712	381	333
Overpayments detected (amount)	$936,488	$499,324	$323,994
Challenges declined	133	47	29
Challenges sustained	105	9	4
Costs	$40,294	$19,028	$36,533

In the reports sent to me, it was noted in the figures that action "was taken without a notice of adverse action" in a surprisingly large number of cases. When my staff queried the reason for this, NZISS advised that these figures were reported in error. NZISS Head Office staff discovered during this year that District Office staff who entered the raw data for the reports did not always appreciate what this category meant and were coding individuals under this category when it did not apply. I have been advised that this problem has been corrected.

NZISS also advised that a notice of adverse action must be issued when adverse action is proposed unless the Head Office staff have been consulted about whether it is appropriate to dispense with a notice. There is a limited category of cases where dispensing with a notice may be appropriate, such as cases to which section 103(2) of the Privacy Act applies, where issuing a notice of adverse action would, for example, "prejudice any investigation into the commission of an offence". NZISS advise that they have received

no such requests since adopting this procedure.

On the basis of the information supplied, I am satisfied that this programme has been conducted in accordance with the requirements of sections 99 to 102 and the information matching rules of the Privacy Act.

IRD/NZISS COMMUNITY SERVICES CARD MATCH

Information matching provision	Tax Administration Act 1994, s.82
Year authorised	1991
Commencement date	1992
Match type	Identification of those eligible for a benefit
Unique Identifiers	Tax file number
On-line transfers	None

The Community Services Card Match is an information matching programme in which Inland Revenue Department supplies NZISS with tax credit information, for the purpose of allowing NZISS to identify those individuals whose income levels are at a level which makes them eligible for a Community Services Card.

There is no adverse action taken as a result of this programme. An individual is offered a Community Services Card if they are successfully matched by the programme.

I have not required any reports from NZISS or IRD for the operation of this programme.

IRD/NZISS COURTS ADDRESS MATCH

Information matching provision	Social Security Act 1964, s.126A
Year authorised	1996
Commencement date	N/A
Match type	Location of persons
Unique Identifiers	None
On-line transfers	None

The NZISS/Courts Address Match is an information matching programme in which the Department for Courts is to be supplied with address information by NZ Income Support Service (NZISS) concerning fines defaulters who receive Income Support. The purpose of the programme is to locate those who owe fines in order to enable recovery of outstanding amounts.

Developments during the year

The Department for Courts sought an amendment to the information matching provision to allow the disclosure of telephone numbers by NZISS. The Department submitted an Information Matching Privacy Impact Assessment to me and I reported to the Minister of Justice on the proposal. In my report, I noted that the telephone numbers held by NZISS were largely inaccurate. However, as plans were in hand to improve the accuracy of that information, the implementing bill was passed by Parliament.

I have been advised that a number of test runs of the new match have taken place. It is not clear whether a reported run dated 15 May 1998 was a "full" run and I am awaiting reports from the Department for Courts. I have been advised that there may be a need for further test runs before the programme is made fully operational.

NZISS/IRD CHILD SUPPORT MATCH

Information matching provision	Tax Administration Act 1994, s.84
Year authorised	1993 (previous tax enactment)
Commencement date	January 1995
Match type	Confirmation of continuing eligibility
Unique Identifiers	Tax file number
On-line transfers	None

The NZISS/IRD Child Support Match is designed to prevent "double-dipping" by those receiving payments of child support from the IRD and Family Support from the NZISS. The two departments compare records of people receiving such payments from NZISS with those receiving such payments from IRD. Where a match is made and confirmed, the IRD payment is ceased. At the end of the tax year overpayments are calculated and appropriate adjustments made.

The benefit from the programme arises because payments of child support by IRD can be stopped upon early detection of those also receiving such payments from NZISS. This saves IRD making payments in error which would later have to be recovered.

Rule 1 compliance

Information matching rule 1 provides that agencies involved in information matching must take "all reasonable steps (which may consist of or include public notification) to ensure that the individuals who will be affected by the programme are notified of the programme." In 1998, IRD

reported to me that they produced a booklet about this matching programme. IRD reported that it did not conduct any other publicity campaign.

Results

Results of the NZISS/IRD Child Support Match for the last three years are as follows.

TABLE 26: NZISS/IRD CHILD SUPPORT MATCH 1996-1998

NZISS/IRD Child Support Match	**1995/96 Runs 6-14**	**1996/97 Runs 15-23**	**1997/98 Runs 24-32**
Cases sent by IRD to DSW for matching *(A)*	658,103	648,438	797,230
Cases sent by IRD to DSW average per run	73,123	81,055	88,581
Cases matched by DSW *(B)*	6,088	6,387	6,297
Cases matched as % of number of cases *(B/A)*	0.92%	0.98%	0.79%
Cases of adverse action taken *(C)*	4,462	5,097	4,927
Cases of adverse action as % of cases matched *(C/B)*	73.3%	79.8%	78.2%
Challenges to notices	28	nil	nil
Challenges successful	22	nil	nil
Savings (estimated) *	$6,244,526	$9,573,428	$12,537,265
Costs reported by DSW as the source agency	$3,592	—	—
Costs incurred by IRD	$300,300	$369,062	$538,017
Total costs	$303,892	$369,062	$538,017

* Calculated by determining the amount of the payments stopped multiplied by the number of weeks left in the financial year (when the payment ought to be stopped/ reviewed because the individual has filed a tax return)

More cases (individual names) were sent to NZISS by IRD for matching this year than in previous years, by a factor of approximately 150,000. However, the number of cases of "double dipping" found was no higher numerically than in previous years, so there is a drop evident in the percentage figure for the comparison of the number of cases of adverse action to the number of cases submitted for matching.

On the basis of the information supplied, I am satisfied that this programme has been conducted in accordance with the requirements of sections 99 to 103 of the Privacy Act and the information matching rules.

NZ IMMIGRATION SERVICE/ELECTORAL ENROLMENT CENTRE MATCH

Information matching provision	Electoral Act 1993, s.263A
Year authorised	1995
Commencement date	August 1996
Match type	• Confirmation of continuing eligibility • Detection of errors
Unique Identifiers	None
On-line transfers	None

The Electoral Match is designed to identify individuals who are enrolled to vote in general elections without the necessary residence qualification. Information is provided by NZ Immigration Service (NZIS) to the Electoral Enrolment Centre (EEC) of all overstayers and visitors who are recorded as being present in New Zealand. From time to time, generally once a year, EEC obtains from NZIS the lists of overstayers and visitors. This information is compared with the electoral roll to identify those who are both enrolled and listed as either visitors to New Zealand or overstayers.

Details of any names matched are sent to the District Registrar of Electors in the electorate in which the individual is enrolled. The matched individuals are sent a notice of adverse action advising that unless proof to the contrary is produced (for example, proof of citizenship) the person may be deleted from the electoral roll. If there is no reply to the notice, a procedure established in section 96 of the Electoral Act is followed. If the individual cannot produce the necessary evidence or does not reply to the notice, he or she is deleted from the electoral roll. If the notice cannot be served, the individual is placed on the "dormant roll" which indicates that their vote will be taken on election day, but it will not be counted unless proof of eligibility to vote is later produced.

Results

TABLE 27: NZ IMMIGRATION SERVICE/ELECTORAL ENROLMENT CENTRE MATCH - NOTICES UNDER SECTION 103 PRIVACY ACT

Section 103 of the Privacy Act – notices	**1996**	**1997**
Letters issued under section 103	315	86
Responses received Voluntarily deleted Retained on roll	63 45 18	26 No figures available No figures available
No response received	252	60

TABLE 28: NOTICES ISSUED UNDER SECTION 96 ELECTORAL ACT

Section 96 of the Electoral Act - notices	1996	1997
Letters issued under section 96 Electoral Act	253	60
Letters actually served	192	47
Responses received Voluntarily deleted Retained on roll	39 27 12	9 13 (1) 9 (1)
No response to Electoral Act letter – deleted from roll	153	25
Letters not served	61 (2)	13
Number placed on dormant roll	57	13
Deleted from roll for other reasons of ineligibility	3	

(1) The decisions made in respect of these individuals may have been before or after the issuing of the section 96 notice.
(2) Including one response to section 103 letter received after issue of section 96 letter.

TABLE 29: EVIDENCE OF ENTITLEMENT TO BE ON ELECTORAL ROLL

Evidence of entitlement to be on the electoral roll	1996	1997
NZ born	2	1
NZ passport	5	0
NZ citizenship	14	2
Permanent residence status	9	6
Total retained on electoral roll	30	9

TABLE 30: RESULTS OF ELECTORAL MATCH

Results of Electoral Match	1996	1997
Retained on Electoral Roll	30	9
Deleted voluntarily	72	13
Deleted involuntarily	156	51
Placed on dormant roll	57	13
Total	315	86

In 1997 the electoral match identified 86 individuals who were on both the Immigration database and the electoral roll. Of those individuals, nine were able to produce proof of eligibility to enrol, which amounts to an "error rate" of 10.5% of those who were identified. In 1996 the error rate was 30 out of 315 cases, or 9.5%. The high error rate is of concern to me.

The number of individuals who were removed from the roll numbered 64. As there were 65 electorates in New Zealand in 1997, this is an average of less than one per electorate. Two electorates had six names deleted, three had five names removed, and 36 electorates had no names removed. A further 13 individuals were placed on the dormant roll, which means that they must produce proof of eligibility to vote after they have cast a special vote but before the vote is counted.

I expressed concerns about this match in last year's annual report and in a report to the Minister of Justice. The right to vote is fundamental in a democratic country. While the stated purpose of the programme, to ensure the integrity of the electoral roll, is important, I am concerned the match may itself be some *threat* to the integrity of the roll because the information exchanged is not sufficiently reliable, thereby removing individuals who might otherwise be entitled to be enrolled. The error rate of 10.5% puts a relatively high proportion of those matched to the trouble of proving their eligibility to enrol.

Recently NZIS advised the EEC that it would be unable to undertake the matching run for 1998. NZIS has indicated that it is not in a position to complete the run, because its new computer programme is still being implemented. EEC, which remains convinced of the worth of the programme notwithstanding the small numbers of discrepancies established, has reluctantly accepted this.

The cost of this programme in 1996 was $30,000. In 1997 the costs were reported to me as $7,523.

Inclusion of visitors in the Electoral Match

In my 1995 report to the Minister of Justice, submitted when the authorising provision was before Parliament, I recommended that consideration be given to excluding visitors from the programme. I referred to the possibility that a visitor could be mismatched with a New Zealander of the same name, which could result in trouble for the legitimate elector. Using only the list of overstayers, the numbers would be smaller and mismatches fewer. Any visitors remaining past the period for which they are entitled to be in New Zealand would be caught at the next run of the matching programme after their status had changed from "visitor" to "overstayer".

The EEC has not separated the reported figures of those matched from the visitors list and from the overstayers list. I therefore have no information as to whether those matched through the programme were visitors or overstayers. This is an issue which needs to be examined next year to see the actual impact of the inclusion of visitors in the programme.

IRD/ACC MATCH

Information matching provision	Accident Rehabilitation Compensation and Insurance Act 1992, ss.164 and 165
Year authorised	1991
Commencement date	1997
Match type	• Confirmation of continuing eligibility • Detection of errors • Detection of illegal behaviour
Unique Identifiers	Tax file number
On-line transfers	None

Last year, I reported that Accident Rehabilitation Compensation and Insurance Corporation (ACC) would commence an information matching programme with the IRD. This information matching programme has been authorised since 1991. The programme was due to commence in August 1997. At about that time ACC did conduct one test run of the programme to obtain employment information for the purpose of detecting individuals fraudulently receiving ACC compensation while also receiving income. The individuals whose names were submitted were from a narrow group of ACC compensation recipients, and I was advised that the run was a test of ACC's systems. Some adverse action was taken. ACC has advised that the match produced some problems which require them to make some fundamental changes which will be reflected in its plans for the next year.

V. Performance and financial statements

STATEMENT OF OBJECTIVES
STATEMENT OF PERFORMANCE
For the year ended 30 June 1998

Output – operations of the Privacy Commissioner

	1998	1997
	$	$
Total cost of producing output	2,082,367	1,942,180

OBJECTIVE 1

- To peruse and report upon proposed legislation.

Performance Indicators

- To peruse proposals for legislation and, having identified those upon which useful input can be made with comments on implications for privacy of the individual, to make those comments where practicable to do so in time for consideration by departments, Ministers or select committees.
- Comments are to be made by the Commissioner or a suitably qualified staff member.

Performance Measures

- Provide comments in respect of proposed legislation within target times set by the Commissioner.

Actual Achievement

- Submissions, reports or comments were made within the target time on all legislative proposals on which the office could usefully comment by the Commissioner or a suitably qualified staff member.

OBJECTIVE 2

- To issue and, as appropriate, review codes of practice.

Performance Indicators

- To consider proposals for codes of practice, provide guidance in the preparation of draft codes and to conduct sector and public consultation, carrying out all tasks by suitably qualified staff and within the time target set by the Commissioner.
- To carry out reviews of all temporary codes issued within one year so as to bring permanent codes into effect (where warranted) as soon as the temporary code expires.

Performance Measures

- Meet all requests for issue of codes within any set target time.
- Complete issue of permanent codes in time for expiry of temporary code.

Actual Achievement

- No temporary codes expired during the period.
- No application was submitted under section 47(2) for a code to be issued by the Commissioner.
- The Justice Sector Unique Identifier Code 1998 was notified, released for public consultation, and issued.
- During the first half of 1998 two proposed amendments to the Health Information Privacy Code 1994 were released for consultation. Neither had been issued by the end of the year.

OBJECTIVE 3

- To handle complaints of interference with privacy.
- To consult with the Ombudsman under the Official Information Act and the Local Government Official Information and Meetings Act.

Performance Indicators

- To receive, notify, investigate and resolve all complaints by use of suitably qualified staff under appropriate supervision as to quality and timeliness.
- To provide comment to the Ombudsman on reviews of the withholding of official information to protect the privacy of natural persons or deceased natural persons.

Performance Measures

- Within the resources of the Office, to undertake all phases of complaints handling with experienced and qualified staff working under appropriate supervision of timeliness and quality.
- To complete the processing of 630 complaints.
- Number of consultations.

Actual Achievement

	Projected	Actual
number of complaints received	1200	1082
number of complaints processed	630	804

- All complaints received by the Office were handled by suitably qualified staff working under supervision and each complaint was subject to full review by the Privacy Commissioner prior to its completion.
- During the year 1,082 complaints were received, jurisdiction assessed and accepted for investigation. Over the same period 804 complaints were resolved or action upon them discontinued and the files closed.
- The number of complaints received was 10% lower than for the previous period. Notwithstanding this, the sustained reduction of resources within the office has continued the growth in the number of complaints held in the queue.
- During the year 77 consultations with the Ombudsmen were completed.

OBJECTIVE 4

- To increase awareness and understanding of the Privacy Act.

Performance Indicators

- To provide enquirers with appropriate information given by suitably qualified staff.
- Within the resources of the Office, to present seminars and workshops to interest groups within the main population centres and elsewhere as warranted.
- To make speeches and other public statements which are of consistently high quality.

Performance Measures

- Numbers of enquiries received and answered by telephone, mail and visits.
- Preparation and issue of printed material to answer routine or general enquiries.
- Numbers and locations of seminars and workshops presented by suitably qualified staff.
- Speeches and public statements made by appropriate staff.

Actual Achievement

	Projected	Actual
number of education/public information programmes	1	1
number of enquiries received	9,000	11,141

- 11,141 enquiries were formally logged. Of these 10,597 telephone enquiries and 9 visits by enquirers were answered. 535 written enquiries were received during the year, of which 429 were answered. Trained staff answered all of these enquiries. In addition there were a number of unrecorded informal enquiries, visits and requests for printed materials which are not formally logged as enquiries.
- Guidance was provided to a number of agencies in more specific terms on the preparation of their own compliance procedures and documents in the course of responding to enquiries and resolving complaints; no separate figures were recorded for this activity.
- Fact sheets prepared by senior staff covering the Act and the Health Information Privacy Code 1994 were supplied on request.
- Regular issues of *Private Word*, the Office newsletter were mailed to a significant proportion of people on the Office mailing lists. The average print run increased to 5,000 copies.
- Three general compilations of material were issued, comprising papers, submissions and speeches. Specialised compilations on Complaints Review Tribunal cases and reports on information matching programmes were also released.
- Mental Health Guidance Notes were produced and widely distributed with the assistance of the Mental Health Commission.
- Work commenced on rebuilding the home page on the Internet to bring it in line with the expectations of users and to make it an integral part of the education programme of the Office.

- Twenty-three case notes were published on the Commissioner's investigations.
- Twenty-six seminars and workshops were presented during the year by qualified and experienced staff of the office.
- A Privacy Issues Forum was held in Auckland and was attended by 158 persons.
- All media statements and the majority of public speeches were made by the Privacy Commissioner personally.

OBJECTIVE 5

- To monitor and report on information matching.
- To review statutory authorities for information matching.

Performance Indicators

- To receive, peruse and question the agreements and periodic reports from agencies undertaking information matching.
- To review and report as soon as practicable after 1 February 1994 on the operation of information matching provisions.

Performance Measures

- Inclusion in the Annual Report of a report on the operation of the information matching programmes during the year.
- Provision of a report to the Minister of Justice on operation of the information matching provisions soon after February 1994.

Actual Achievement

- A full report on the information matching programmes operated in the year 1997/98 is contained in this annual report.
- There was a failure to meet the performance measure in relation to the provision of a report to the Minister of Justice on operation of the information matching provisions. Work on that review commenced in the 1996/97 year and continued during the 1997/98 year but is not yet complete. It is intended to stage completion of the required reports and to have the first batch or batches completed before the end of the 1998/99 year.

PRIVACY COMMISSIONER
STATEMENT OF FINANCIAL POSITION
As at 30 June 1998

1996/97 $		1997/98 $	1997/98 Budget/$
	CURRENT ASSETS		
450	Cash on Hand	450	450
98,082	Short term deposits	53,730	16,517
11,596	Debtors	14,811	11,596
-	Inventory	20,788	-
5,986	Prepayments	5,658	5,986
116,114	**TOTAL CURRENT ASSETS**	**95,437**	**34,549**
	NON CURRENT ASSETS		
151,621	Fixed Assets (note 2)	87,946	141,621
267,735	**TOTAL ASSETS**	**183,383**	**176,170**
	CURRENT LIABILITIES		
138,509	Sundry Creditors (note 1)	233,575	138,509
129,226	**NET ASSETS**	**(50,192)**	**37,661**
129,226	**EQUITY**	**(50,192)**	**37,661**

B H Slane
Privacy Commissioner

30 October 1998

The accompanying notes and accounting policies form an integral part of these financial statements.

PRIVACY COMMISSIONER
STATEMENT OF FINANCIAL PERFORMANCE
For The Year Ended 30 June 1998

1996/97 $		1997/98 $	1997/98 Budget/$
	INCOME		
1,764,444	Operating Grant	1,764,444	1,764,444
83,403	Other Income	120,118	83,080
33,087	Interest	18,387	15,000
1,880,934	**TOTAL INCOME**	**1,902,949**	**1,862,524**
	EXPENSES		
26,530	Marketing/Newsletter	56,778	64,000
6,000	Audit Fees	6,500	6,000
58,867	Depreciation	65,170	35,000
—	Rental Expense	171,901	171,000
727,892	Operating expenses	657,848	573,529
1,122,891	Staff Expenses	1,124,170	1,129,560
1,942,180	**TOTAL EXPENSES**	**2,082,367**	**1,979,089**
(61,246)	**NET SURPLUS (DEFICIT)**	**(179,418)**	**(116,565)**

The accompanying notes and accounting policies form an integral part of these financial statements.

PRIVACY COMMISSIONER
STATEMENT OF CASH FLOWS
For the Year Ended 30 June 1998

1996/97 $		1997/98 $	1997/98 Budget/$
	Cash Flows from Operating Activities:		
1,764,444	Government Grant	1,764,444	1,764,444
81,467	Other Income	99,718	83,080
33,087	Interest	18,387	15,000
1,878,998		**1,882,549**	**1,862,524**
	Cash was applied to:		
670,237	Payments to Suppliers	881,375	789,529
1,134,257	Payments to Employees	1,103,143	1,129,560
166,808	Payments of GST	(59,112)	—
1,971,302		**1,925,406**	**1,919,089**
(92,304)	**Net Cash Flows applied to operating activities**	**(42,857)**	**(56,565)**
	Cash Flows from Investing Activities		
	Cash was applied to:		
89,231	Purchase of Fixed Assets	1,495	25,000
(89,231)	**Net Cash Flows applied to Investing Activities**	**(1,495)**	**(25,000)**
(181,535)	**Net Decrease in Cash Held**	**(44,352)**	**(81,565)**
280,067	**Cash Brought Forward**	**98,532**	**98,532**
98,532	**Closing Cash Carried Forward**	**54,180**	**16,967**
	Cash Made up of:		
450	Cash on Hand	450	450
20,558	Countrywide Bank	31,717	16,517
77,524	Countrywide Bank - Deposit	22,013	—
98,532		**54,180**	**16,967**

The accompanying notes and accounting policies form an integral part of these financial statements.

RECONCILIATION OF CASH FLOWS FROM OPERATING ACTIVITIES

1996/97 $		1997/98 $	1997/98 Budget/$
(61,246)	Excess Expenses over Income	(179,418)	(91,565)
	Non-Cash Item		
58,867	Depreciation	65,170	35,000
	Movements in Working Capital		
(87,651)	Increase (Decrease) in Creditors	95,066	—
(338)	Decrease (Increase) in Prepayments	328	—
—	Increase in Inventory	(20,788)	—
(1,936)	Increase in Debtors	(3,215)	—
(92,304)	.....	**(42,857)**	**(56,565)**

STATEMENT OF MOVEMENTS IN EQUITY
As At 30 June 1998

1996/97 $		1997/98 $
190,472	Equity at 1 July 1997	129,226
(61,246)	Excess of Expenses over Income for the year	(179,418)
(61,246)	Total recognised Revenue and Expenses for the year	(179,418)
129,226	Equity at 30 June 1998	(50,192)

The accompanying notes and accounting policies form an integral part of these financial statements.

PRIVACY COMMISSIONER
STATEMENT OF ACCOUNTING POLICIES
For the Year Ended 30 June 1998

1. ACCOUNTING POLICIES

1.1 Reporting Entity

The Privacy Commissioner is a crown entity as defined by the Public Finance Act 1989.

These are the financial statements of the Privacy Commissioner prepared pursuant to Sections 41 and 42 of the Public Finance Act 1989.

1.2 Measurement Base

The general accounting systems recognised as appropriate for the measurement and reporting of results and financial position on an historical cost basis have been followed.

2. SPECIFIC ACCOUNTING POLICIES

2.1 Budget Figures

The Budget figures are those adopted by the Privacy Commissioner at the beginning of the financial year. The budget figures have been prepared in accordance with generally accepted accounting practice and are consistent with the accounting policies adopted by the Commissioner in the preparation of the financial statements.

2.2 Revenue

The Privacy Commissioner derives revenue from the provision of services to Parliament, for services to third parties and interest on its deposits. Such revenue is recognised when earned and reported in the financial period to which it relates.

2.3 Debtors

Debtors are stated at their expected realisable value.

2.4 Leases

Operating lease payments, where the lessor effectively retain substantially all the risks and benefits of ownership of the leased item are charged as expenses in the periods in which they are incurred.

2.5 Fixed Assets

Fixed Assets are stated at their cost price less accumulated depreciation.

2.6 Depreciation

Fixed Assets are depreciated on a straight-line basis over the useful life of the asset. The estimated useful lives are:

Furniture and Fittings	5 Years
Office Equipment	5 Years

2.7 Employee Entitlements

Provision is made in the financial statements for the Privacy Commissioner's liability in respect of annual leave. Annual leave has been calculated on an actual entitlement basis at current rates of pay.

The total remuneration of the Privacy Commissioner was $154,100

2.8 Financial Instruments

The Privacy Commissioner is party to financial instruments as part of its normal operations. These financial instruments include bank accounts, short-term deposits, debtors and creditors. All financial instruments are recognised in the Statement of Financial Position and all revenue and expenses in relation to financial instruments are recognised in the Statement of Financial Performance.

2.9 Goods and Services Tax

The financial statements are shown exclusive of GST. The amount of GST owing to or from the Inland Revenue Department at balance date, being the difference between output GST and input GST, is included as either a debtor or creditor (as appropriate).

2.10 Commitments

Future expenses and liabilities to be incurred on contracts that have been entered into at balance date are disclosed as commitments to the extent that these are equally unperformed obligations.

2.11 Contingent Liabilities

Contingent liabilities are disclosed at the point that the contingency is evident.

2.12 Inventory

Publications inventory held for sale is valued at the lower of cost, determined on a first in first out basis, or net realisable value.

3. CHANGES IN ACCOUNTING POLICIES

There have been no changes in Accounting Policies since the date of the last audited financial statements.

PRIVACY COMMISSIONER
NOTES TO THE FINANCIAL STATEMENTS
For the Year Ended 30 June 1998

1. SUNDRY CREDITORS

1996/97 $		1997/98 $
82,733	Accruals - Wages and Holiday pay	91,800
50,343	Trade Creditors	73,393
5,433	GST	68,382
138,509	**TOTAL SUNDRY CREDITORS**	**233,575**

2. FIXED ASSETS

	Cost/$	1996/97 Accum Depn/$	Closing Bk Val/$	Cost/$	997/98 Accum Depn/$	Closing Bk Val/$
Office Equipment	276,318	144,421	131,897	277,813	199,984	77,829
Furniture and Fittings	48,038	28,314	19,724	48,038	37,921	10,117
	324,356	172,735	151,621	325,851	237,905	87,946

3. OPERATING COMMITMENTS

1996/97 $		1997/98 $
152,069	Less than one year	161,243
89,026	one - two years	123,588
83,914	two - five years	104,760
—	greater than five years	—
325,009		**389,591**

Note: Commitments are based on leave costs prior to rent reviews on 1/7/98. The rent reviews indicated an overall increase in commitments of $210,000. This increase is currently in dispute.

4. CONTINGENT LIABILITIES

1996/97 $		1997/98 $
Nil	Contingent Liabilities	Nil

5. CAPITAL COMMITMENTS

1996/97 $		1997/98 $
Nil	Capital Commitments	Nil

6. FINANCIAL INSTRUMENTS

The Privacy Commissioner is party to financial instruments as part of its normal operations. These financial instruments include bank accounts, short term deposits, debtors, and creditors.

6.1 CREDIT RISK

Credit risk is the risk that a third party will default on its obligations to the Privacy Commissioner, causing the Commissioner to incur a loss. In the normal course of its business the Commissioner incurs credit risk from debtors and transactions with financial institutions. The Privacy Commissioner does not generally require security from debtors. The maximum exposure to credit risk at the 30 June 1998 is: -

1996/97 $		1997/98 $
98,082	Bank Balances	53,730
11,596	Debtors	14,811
109,678		**68,541**

STATEMENT OF RESPONSIBILITY

In terms of Section 42 of the Public Finance Act 1989.

1. I accept responsibility for the preparation of these financial statements and the judgements used therein, and
2. I have been responsible for establishing and maintaining a system of internal control designed to provide reasonable assurance as to the integrity and reliability of financial reporting, and
3. I am of the opinion that these financial statements fairly reflect the financial position of the Office of the Privacy Commissioner for the period ended 30 June 1998.

B. H. Slane
Privacy Commissioner

Audit New Zealand

REPORT OF THE AUDIT OFFICE

TO THE READERS OF THE FINANCIAL STATEMENTS OF THE PRIVACY COMMISSIONER FOR THE YEAR ENDED 30 JUNE 1998

We have audited the financial statements on pages 100 to 112. The financial statements provide information about the past financial and service performance of the Privacy Commissioner and its financial position as at 30 June 1998. This information is stated in accordance with the accounting policies set out on pages 109 to 110.

Responsibilities of the Privacy Commissioner

The Public Finance Act 1989 requires the Privacy Commissioner to prepare financial statements in accordance with generally accepted accounting practice which fairly reflect the financial position of the Privacy Commissioner as at 30 June 1998, the results of its operations and cash flows and the service performance achievements for the year ended 30 June 1998.

Auditor's Responsibilities

Section 43(1) of the Public Finance Act 1989 requires the Audit Office to audit the financial statements presented by the Privacy Commissioner. It is the responsibility of the Audit Office to express an independent opinion on the financial statements and report its opinion to you.

The Controller and Auditor-General has appointed B H Halford, of Audit New Zealand, to undertake the audit.

Basis of Opinion

An audit includes examining, on a test basis, evidence relevant to the amounts and disclosures in the financial statements. It also includes assessing:

- the significant estimates and judgements made by the Commissioner in the preparation of the financial statements; and
- whether the accounting policies are appropriate to the Privacy Commissioner's circumstances, consistently applied and adequately disclosed.

We conducted our audit in accordance with generally accepted auditing standards in New Zealand. We planned and performed our audit so as to obtain all the information and explanations which we considered necessary in order to provide us with sufficient evidence to give reasonable assurance that the financial statements are free from material misstatements whether caused by fraud or error. In forming our opinion, we also evaluated the overall adequacy of the presentation of information in the financial statements.

Other than in our capacity as auditor acting on behalf of the Controller and Auditor-General, we have no relationship with or interests in the Privacy Commissioner.

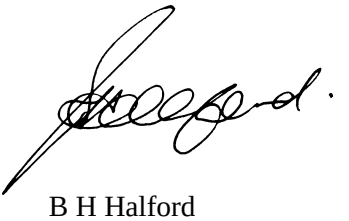
Unqualified Opinion

We have obtained all the information and explanations we have required.

In our opinion the financial statements of the Privacy Commissioner on pages 100 to 112:

- comply with generally accepted accounting practice; and
- fairly reflect:
  - — the financial position as at 30 June 1998;
  - — the results of its operations and cash flows for the year ended on that date; and
  - — the service performance achievements in relation to the performance targets and other measures adopted for the year ended on that date.

Our audit was completed on 30 October 1998 and our unqualified opinion is expressed as at that date.



B H Halford
Audit New Zealand
On behalf of the Controller and Auditor-General
Auckland, New Zealand

Privacy Commissioner
Te Mana Matapono Matatapu

Auckland Office
PO Box 466, Auckland
Telephone 09-302 8680
Facsimile 09-302 2305
Privacy enquiries 09-302 8655
Email privacy@iprolink.co.nz

Wellington Office
PO Box 10-094, Wellington
Telephone 04-474 7590
Facsimile 04-472 7595
Email privacy@actrix.gen.nz

Privacy Hotline
0800 803 909

Internet address
http://www.privacy.org.nz