Privacy Commissioner
Te Mana Matapono Matatapu

Report of the Privacy Commissioner

for the year ended 30 June 2000

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

Privacy Commissioner
Te Mana Matapono Matatapu

Report of the Privacy Commissioner

for the year ended 30 June 2000

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

Letter to Minister

November 2000

Hon Phil Goff MP
Minister of Justice
WELLINGTON

I tender my report as Privacy Commissioner for the year ended 30 June 2000.

B H Slane
Privacy Commissioner

Contents

Tables and Figures

Complaints

Enquiries

Functions Under Other Enactments

Information Matching

Figures

I. Introduction

Access is important

The ability to access one's own personal information when held by a business or a government agency is not always accepted by those agencies as a fundamental or basic right in our society. Too often I hear agencies asking why the person would want to access that material. That is not the issue. Parliament has given people the right to request access to their own information and has given a limited number of grounds on which agencies may refuse to make that information available. It is a pervasive right.

No longer is personal information simply gathered into files which themselves gather dust. It usually forms part of an electronic database where it can be accessed, manipulated, used, developed or - if care is not taken - abused, exploited, extracted or deleted by people not entitled to do so.

Often personal information is being used to make decisions about people without those very people being aware that use is being made of it. If information records are scrupulously accurate, relevant and up-to-date they support good decision making.

I see the role of the individual as first auditor of the databanks they voluntarily or involuntarily belong to. They can confirm its accuracy and relevance – and seek correction if it is wrong.

Sometimes people's requests for their information are treated in a cavalier fashion or they are simply neglected. Perhaps a cursory search is made or little more. I have referred cases to the Proceedings Commissioner. Most of them proceed to the point of settlement, or a successful judgment.

Remedies for breaches

It was heartening to read the judgment of the High Court led by Justice Smellie in the case *Proceedings Commissioner v Health Waikato*. The judgment in part reads:

> *A citizen can be as difficult, unreasonable and reprehensible as one can possibly imagine, but if his or her privacy rights have been breached and additional stress suffered in an already stress-*

ful situation, then those unattractive characteristics have no part to play in deciding whether or not damages should be awarded in compensation.

In that case the Court ordered damages of $8,000 and costs of $5,500 to be paid to the individual concerned, $5,000 of which was for not getting "a fair crack of the whip" when Health Waikato failed to disclose information that would have been useful to a former employee in grievance proceedings before the Employment Tribunal.

The Complaints Review Tribunal decided the delay had caused an interference with the employee's privacy, but did not award damages. The Tribunal's decision was influenced by the view that the employee was primarily responsible for the deterioration of the employment relationship and the permanent tension in the relationship had contributed to the errors.

Taxpayer rights

There are still some pockets of resistance to the right of access to one's own personal information. It is interesting that the matter was considered by the Finance and Expenditure Committee of the House of Representatives. (See discussion under Part III of this report, Legislation: Tax Administration Act.)

I was pleased to observe that the Finance and Expenditure Committee had accepted that the procedures of the Privacy Commissioner and the Complaints Review Tribunal should be available to taxpayers who believed they had not received what they were entitled to under principle 6. At present, access rests on the discretion of the Commissioner of Inland Revenue which in practice means the discretion of some tax official further down the Department.

The Finance and Expenditure Committee rejected an alternative of dealing with these matters under the Official Information Act which would have provided under the procedures of the Ombudsmen no access to enforceable remedies and no right to compensation for losses incurred, or damage suffered, as a result of the wrongful withholding of information or undue delay.

The right to ask for the reasons for a decision by the department under the Official Information Act is in practice of limited efficacy. In most of the cases which we see and where we raise this issue with

a taxpayer, the taxpayer shows little interest in getting a formal list of reasons as they already know the basis of the decision. What they want to see is the information on which that decision was based. Only principle 6 can achieve that as a taxpayer right. In the case of a corporate taxpayer, the mirror provisions in Part IV of the Official Information Act would give no right of compensation for corporate taxpayers if that provision were to continue to apply rather than principle 6.

While a department may think it best to resist such impediments on its power, small though they might seem, exercising rights rather than being supplicants is important for taxpayers who, after all, are the ultimate owners of the Inland Revenue Department. It is to be hoped that the Government will not be persuaded, because of the risk of having to pay damages for errors or delays by the Department, from allowing the exercise of rights available in respect of other Government departments. There is no basis for the IRD to be treated differently.

These cases illustrate the advantage that individuals now have through the Privacy Act: the appeal courts have determined that in extreme cases the level of damages can be substantial because there has been real harm and a person has not had what they are entitled to and have suffered as a result.

However, I am pleased to observe that most access complaints that reach this office are quickly dealt with by the agency concerned once we have been in touch with them.

A day in court

I had previously signalled that I intended to invite some complainants to go directly to the Complaints Review Tribunal. Normally I would investigate such cases. This was an attempt to try to reduce the numbers waiting about 18 months for a full investigation. As is explained in the complaints section of this report, half of the cases are dealt with by managers and a case management officer, to bring about a resolution without the need for the case to be taken up by an investigating officer. The consequence is that the remaining cases are waiting a considerable period for a resolution. In some cases there may be a question of credibility, in other cases there may be a point of law which could usefully be determined, and in a few, there may not be great substance in the complaint although only an investigation would make that clear. Unfortunately

although we had persuaded many people to refer cases to the Tribunal, and some did so without the assistance of legal representation, a significant proportion of these proceedings were struck out and the evidence not heard. This may lead complainants to conclude that the system has denied them a hearing of their case.

I happen to believe that our process of a private investigative procedure backed by the right to resort to an adversarial hearing, is an excellent cost-effective process. However, it does depend on a few people getting their "day in court" which is an important part of citizens' acceptance of justice in those cases where it may not seem to have been done to them.

Investigation and resolution

A key element of the high rate of resolution of cases in this office is the power of the Commissioner to investigate. In many cases, it is only when the investigatory powers start to produce answers, witnesses, documents and other leads to the truth of the matter that the parties realise that there is value in trying to come to a conciliated settlement or indeed to accept that their side of the case is not likely to succeed.

One advantage of the process is that there is no public judgment from a judicial body, there is no public airing of their personal life, and very often there is a resolution with which both parties can live. The compliance cost of this procedure for agencies is dramatically lower than would be encountered if an adversarial or litigation model alone were followed. This office is much aided by many lawyers who make representation, present evidence, seek out facts to support the position of their client and generally aid our investigation.

Systemic inquiries

The role of the office is not one where compliance is led by investigating complaints. Complaints lead to more systemic investigations, rather than efforts to resolve a single complaint and do nothing more. There is a wider approach addressed by the procedures of this office which enables me to tackle systemic issues. At the close of the year, there were eight formal inquiries, or own motion investigations, being undertaken by this office. Such inquiries take considerable time and resources and are not lightly undertaken. If they appear to be leading nowhere the inquiry is

stopped. Where however they produce some information of general use, the results can be made public and lessons can be learned.

I believe the approach we are taking will have an effect on the level of complaints received in the future.

We have encountered difficulties with only one government department which persistently defends cases brought whether they appear to have merit or not. I consider this speaks well of agencies' general desire to comply with the Act. During the year I contacted the one department about the degree of training that was being undertaken and although promises to take some action in this respect were expressed, the results were not evident at the close of the year. The matter is being followed up. A number of other departments have taken up training opportunities with a good effect.

However, in one case investigated during the year I was surprised to find that a local body-financed organisation was expending considerable sums in legal advocacy to try and support the withholding of information by a government department when I considered there was no basis for doing so. I think there is a case for naming respondents and the associated organisations in cases of this kind, so that taxpayers and ratepayers may question the cost of work that has been put in to resisting a person's rights of access to their own information, or in fighting other complaints which ultimately do not appear to have any merit.

European Union

I have been pleased that towards the end of the year the new Government decided to pursue the legislative changes I had recommended nearly two years ago, to enable New Zealand traders to have a competitive edge when doing business in Europe. The European Commission will be announcing a white-list of countries whose laws are considered adequate across the board so that there will be no impediment to cross-border flows of personal data from those countries. At the end of the year the amendments were awaiting all party support so they could be included in a non-controversial statutes amendment bill.

I have been surprised that business interests have not seen the advantage of pressing for changes to be made. One can only wonder whether all the opportunities for trading with Europe are being utilised, particularly in the growing field of electronic commerce

and outsourcing work such as overnight translations. It is appropriate therefore that government initiatives are taken to promote the growth of New Zealand enterprise in these vital areas as the world changes. I will be trying to show New Zealand companies that a prominent display of privacy statements and consumer rights on their websites will be good for business. All the evidence from the United States points to lack of confidence or trust as the greatest impediment to consumer buying on the Internet. The principal concern is that the customer's personal information will not be safe and if something goes wrong there will be no possible remedy. In relation to New Zealand web sites the legal position for consumers is much better than in the United States and we should be proud to say so.

II. Office and Functions of the Privacy Commissioner

The Privacy Commissioner is independent of the Executive. This means 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 that 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 an enquiries team available to answer questions and have for several years maintained a toll free enquiries line so that

people may make enquiries without charge from anywhere in New Zealand. This service has had to be restricted and many callers must now leave messages, which are usually responded to within one or two days.

As part of my educative role, I maintain 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. It is a powerful tool for my office, and many enquirers are directed to it for the information they require.

Staff from my office conduct regular workshops and seminars including half-day introductions to both the Privacy Act and the Health Information Privacy Code and a full day workshop aimed at the mental health sector. I also offer tailored workshops that are adapted to the organisation involved. I 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. A code of practice can modify the information privacy principles by:

- prescribing standards that are more or less stringent than those 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 that 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 that compete with privacy.

Other functions of the Privacy Commissioner are found in section 13 of the Act and 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.

In last year's report, I commented on the need for a simple legislative amendment to enable New Zealand to comply with the European Union Directive on Data Protection. This has yet to eventuate, but I remain convinced that it would be of benefit both for trade and privacy reasons.

STAFF

At 30 June 2000 the following staff were employed in the Auckland and Wellington offices.

Susan Allison	Librarian (part-time)
Marilyn Andrew	Support staff (part-time)
Brent Carey	Investigating officer
Eleanor Cooley	Support staff
Bernard Darby	Privacy policy officer (part-time)
Terry Debenham	Enquiries officer
Ina de Polo	Support staff
Michelle Donovan	Investigating officer
Antonia Dowgray	Investigating officer
Annabel Fordham	Executive officer
Margaret Gibbons	Support staff
Fred Henderson	Enquiries officer
Sandra Kelman	Senior investigating officer/Education officer
Kristin Langdon	Complaints team leader

Eve Larsen	Support staff
Ian MacDonald	Senior enquiries officer
Tania Makani	Complaints management officer
Deborah Marshall	Manager, Investigations
Sharon Newton	Support staff
Glenda Osborne	Accounts clerk (part-time)
Kimberley Parkin	Investigating officer
Wendy Proffitt	Privacy policy officer
Carolyn Richardson	Investigating officer
Sue Rodgers	Support staff (part-time)
Tony Sauri	Data matching compliance officer
Jacci Setefano	Investigating officer
Amir Shrestha	Support staff
Blair Stewart	Assistant Commissioner

I have also been well served by **Gary Bulog**, **Robert Stevens**, **Graham Wear** and **Shane Clapson** who have been variously involved in management, legal, advising, information matching and publication projects for me.

III. Report on Activities

CODES OF PRACTICE

Under Part VI of the Privacy Act, I may issue codes of practice in relation to agencies, information, activities, industries, professions and callings. Codes may also be issued under Part VII in relation to public registers. I issued no new codes of practice during the year but the following codes, issued under Part VI in previous years and reported on in earlier annual reports, remained in force:

- Health Information Privacy Code 1994;
- Superannuation Schemes Unique Identifier Code 1995;
- EDS Information Privacy Code 1997;
- Justice Sector Unique Identifier Code 1998.

Amendments to Health Information Privacy Code 1994

Amendments No 4 and 5 to the code were issued during the year. The principal purposes of both amendments were to make technical changes arising from changes in other legislation and to extend the application of the code to certain new categories of agency.

Amendment No 4 was issued on 1 March 2000. It reflected the then Government's changes to the public health system and workplace accident compensation regime (a number of elements of which were later reversed, or are to be reversed, by the new Government). In particular, the accident insurance arrangements created new roles for insurance companies and "exempt employers" which were reflected in the application of the code.

The amendment also applied the code to the Department for Courts, in its capacity of holding sensitive medical records following the completion of inquests, and to pharmaceutical companies. Rule 3(4)(a) of the code, which allowed for non-compliance with rule 3(1) with the authorisation of the individual concerned, was revoked. This change was consistent with a recommendation I made in my review of the operation of the Privacy Act. Amendment No 4 also permitted several more health agencies to assign the National

Health Index Number in circumstances where that would otherwise breach rule 12(2) and made a number of other technical amendments.

Amendment No 5 made further technical amendments to the code. In anticipation of a major republication of the code the opportunity was also taken to "tidy up" certain provisions (through consolidation and reordering) so as to make them more convenient for users of the new reprint.

Amendment No 5 made an important substantive change in the area of complaints handling. A new clause was introduced which required most health agencies, including all health and disability service providers, to have internal complaints procedures which meet certain standards and time limits. The requirement to have an internal complaints procedure is also a requirement of the Code of Health and Disability Services Consumers' Rights and in general the clause is modelled on the "right to complain" in that code. It is my hope that the internal processes will provide a satisfactory means of resolving certain complaints internally without my involvement in many instances. It also encourages agencies to "own the problem" where things go wrong in their agency. However, the existence of internal complaints processes does not affect an individual's right to complain directly to my office.

New edition of Health Information Privacy Code

Given the significance of health information and the nature of privacy issues arising in the health sector, the Health Information Privacy Code has been an important document since it was first released as a temporary code in 1993. The code has been well received by the health sector. One of the reasons for this is the explanatory commentary and other helpful material, such as extracts from statutes, which are published with the code.

Although the commentary to the code has stood the test of time and continues to be accurate and helpful, I decided to revise the booklet taking into account experience from the last six years. The new edition, incorporating all of the amendments issued to date and thoroughly redesigned, was made available prior to Amendment No 5 coming into force.

Prolonging of EDS Information Privacy Code 1997

During the year I amended the EDS Information Privacy Code 1997. The principal purpose of the amendment was to extend the life of the code from 30 June 2000, when it was otherwise due to expire, for three years. This was to ensure that during that period a private company, EDS (New Zealand) Ltd, which operates the computer facilities which process certain government information, will not be permitted to transfer the information outside New Zealand for processing without the express consent of the relevant government department. Any such consent is required to be notified to the Privacy Commissioner with an explanation of the data protection safeguard to be taken.

The code continues an arrangement commenced with the GCS Information Privacy Code 1994. I issued that code in anticipation of the privatisation of GCS Ltd (formerly known as the Government Computing Service). That company operated, amongst other things, the Wanganui Computer and the IRD computer. Prior to the expiry of the 1994 code, I determined that there was a continuing need for controls of the type established in that code and accordingly issued the 1997 code. A limited term was given to the 1997 code in order that the matter be reconsidered at a later date in case circumstances had significantly changed rendering the code unnecessary.

I took the position that the code was not, as yet, unnecessary and undertook consultation with agencies affected by it. Following completion of that informal consultation I publicly notified the proposed amendment to extend the life of the code and considered the submissions received. The amendment was issued on 11 April 2000 and came into effect on 1 June deleting the existing expiry date and substituting 30 June 2003. The opportunity was also taken to update the schedule of agencies to which the code applies, to delete those that were no longer clients of EDS and to substitute new names for certain government agencies.

Proposals for two new codes: telecommunications and credit reporting

During the year I recommenced work on two longstanding proposals for codes of practice in the areas of credit reporting and telecommunications. It had not been possible to progress these projects in the last few years, notwithstanding that certain industry compa-

nies had presented draft codes to me several years ago. I engaged a staff member on a limited term contract to work exclusively on these two projects.

I commissioned the preparation of a resource document on privacy issues in telecommunications. *Privacy on the Line: a resource document in relation to privacy in telecommunications* was prepared by Nigel Waters, a privacy expert from Australia, and staff from my office. The document was completed and made publicly available shortly after the end of the year and is freely accessible on my website. The paper explains what is special about telecommunications and delves into a variety of issues. I believe that the document will be a valuable resource at a later date when a draft code is released and public consultation is undertaken.

In-house work was undertaken in preparing a draft code of practice for credit reporting. Two proposed codes of practice given to me several years ago by parties involved in credit provision and reporting are a major resource in preparing that draft, as is the approach taken in other jurisdictions with similar privacy laws (including a code of practice for credit reporting produced under the Hong Kong privacy law, which was not available when the industry drafts were prepared).

It is my intention to bring both code proposals to the stage of public consultation and possible issue in 2001.

COMPLAINTS

Complaints received

Table 1 shows the complaints received and closed during the year. I received fewer complaints than last year. As I will discuss later in the report, the lack of resources provided to my office for complaints has meant that complaints have to be placed in a "queue" system and towards the end of the year there was an 18 month delay between receiving a complaint and assigning an investigating officer. The delay accounts for some of the lower level of complaints received. Given the delay people may be discouraged from making a complaint as it is not seen as an effective remedy.

Increasingly agencies are managing their Privacy Act obligations effectively. Many of the privacy officers who deal with my office are becoming increasingly familiar with the Act and the obligations it places on their agency. Policies, processes and staff training result in fewer complaints to my office as people approaching agencies will be given the response they are entitled to under the Act and fair information practices then established.

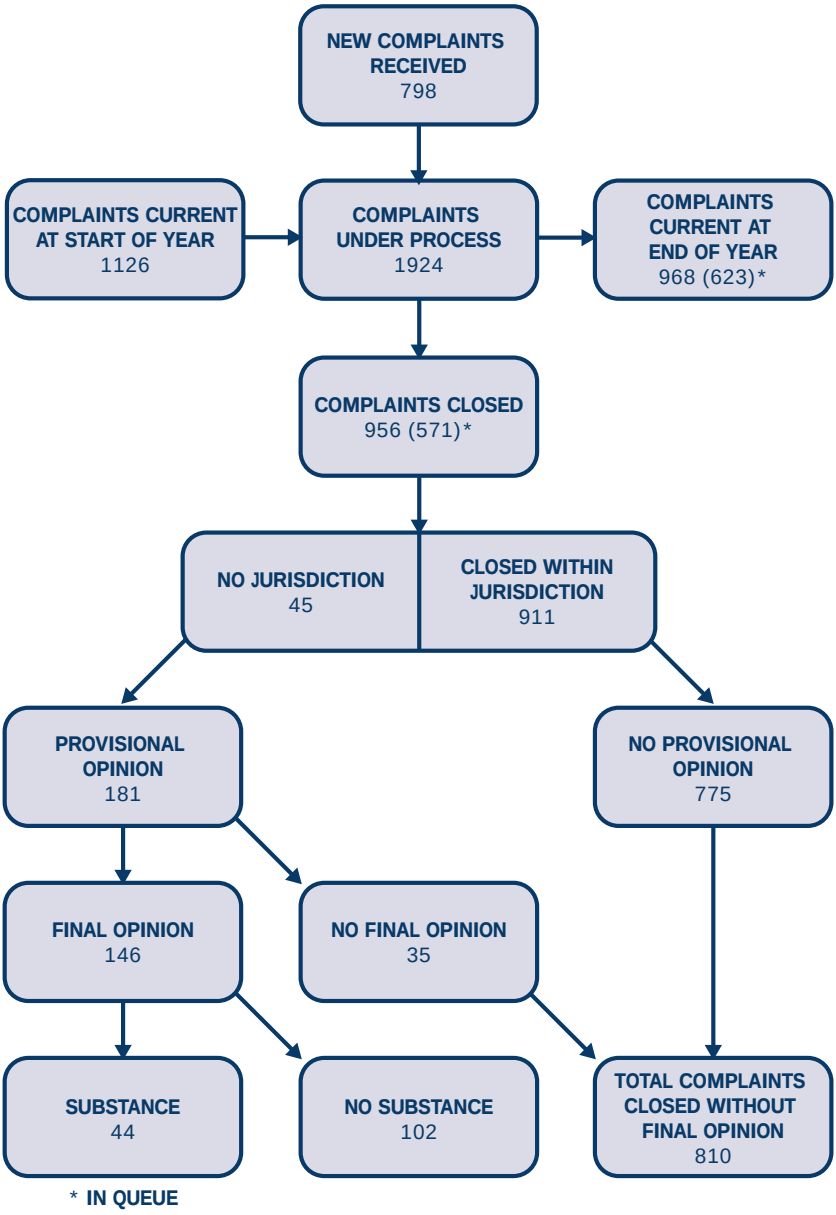
TABLE 1: COMPLAINTS RECEIVED AND CLOSED 1995-2000

	1994/95	1995/96	1996/97	1997/98	1998/99	1999/00
Complaints received	877	993	1200	1088	1003	798
Complaints closed	633	972	870	804	895	956

Figure 1 (page 23) represents the flow of incoming complaints and the complaints disposed of during the financial year.

During the year 798 new complaints were received. At the end of the year, 968 complaints were current (under investigation). Of those, 623 were in the queue waiting to be assigned to an investigating officer. In July 1999 the queue reached a peak of 830. As a result of an increase in my funding I was able to employ more investigating staff and the queue has reduced from that high of 830 to 623 at the end of the year.

FIGURE 1: COMPLAINTS 1999/2000



Complaints in the queue are not left idle. During the year I appointed a Complaints Management Officer, who deals with the queued complaints in an effort to resolve them informally before assignment to an investigating officer. She is assisted in this by the Investigations Manager and Complaints Team Leader. During the year, 571 of the completed complaints were closed in the queue without being assigned to an investigating officer.

Less than 5% of complaints were closed because they were outside my jurisdiction, indicating that most complainants are aware of the nature of my jurisdiction. I have encountered no confusion in the minds of the public as to where to go to have a privacy complaint dealt with.

It was possible to resolve 85% of complaints within my jurisdiction without forming a final opinion. This is consistent with figures from previous years. It indicates the willingness of parties to reach a conclusion acceptable to both with the skilled assistance of my investigating staff. However, I am satisfied that the power to investigate and to require answers to questions during investigation is a vital element in securing such a high rate of conciliated resolutions.

Investigation of complaints

Complaints not resolved while in the queue are eventually assigned to an investigating officer.

Because so many of the complaints are resolved without being assigned to an investigating officer, the complaints that remain to be investigated are more difficult to resolve. They generally raise more complex legal issues, where the facts are hard to establish, or where the parties have reached a position where settlement is unlikely. This has resulted in a drop in the number of complaints completed by each investigating officer.

However, many of the complaints investigated can be settled without the need for me to form a final opinion on the substance of the complaint. In my experience as the investigation progresses and the facts become clear it is easier to point to the likely result of proceeding further. This often persuades an otherwise adamant party that their position is untenable and this insight leads to settlements. 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 a 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 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 compensation or some other restorative action being undertaken.

Some examples of settlements achieved during the year are as follows:

- An agency disclosed to the complainant's father details of the complainant's hire purchase arrangement and the fact that the payments were in arrears. The agency paid $3,000 to the complainant and apologised for the disclosure.

- A $20,000 settlement was made for breaches of rules 1, 2, 4 and 8 of the Health Information Privacy Code. The circumstances leading to these breaches involved a visit by a mental health team to the complainant's property as a result of a telephone call to the team from a neighbour.

- A complaint about an agency in breach of principle 6 for failing to respond to a man's request for access to complaints made about him was settled by a $9,000 payment to charities nominated by the complainant.

- A telecommunications agency disclosed to a flatmate details of a debt owed by the complainant. This resulted in the flatmates falling out and the dissolution of the flatting arrangement. The agency involved forgave the $1200 debt as settlement of the complaint of disclosure.

Complaints involving access to information are often resolved once the individual receives the information requested. In other cases, the delay in getting access may have caused some loss to the requester.

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 other cases the agency realises as the investigation proceeds that it is in breach and takes steps to resolve the complaint. In those cases I may discontinue my investigation without forming a provisional opinion.

If settlement is not achieved, I may give my provisional opinion on the complaint. That may serve to resolve the complaint so that settlement can be achieved at that stage. During the year I formed a provisional opinion on 19% of complaints closed and in 15% I went on to form my final opinion. Clearly this process results in some settlements and avoids the need for litigation. Even where I have formed a final opinion, I will usually try to attempt a settlement.

Complaints involving access

The right of access to personal information is an important right. It increases accountability in public and private sector agencies. Once access has been obtained, the individual has a right to request that information be corrected and this helps to ensure that decisions affecting people are made on the basis of accurate and up-to-date information.

Access complaints differ from other complaints in that the complainant cannot know whether the request has been properly complied with. My office can review a decision not to make some or all of the personal information available to a requester. Figures for access complaints are taken from those complaints that are closed within jurisdiction and involve access. These complaints may also involve alleged breaches of other principles as well as principle 6.

TABLE 2: COMPLAINTS INVOLVING ACCESS BY SECTOR 1995-2000

	1994/95	1995/96	1996/97	1997/98	1998/99	1999/00
Private Sector	150	176	256	170	148	142
Public Sector	218	181	206	179	212	241
Total	**368**	**357**	**462**	**349**	**360**	**383**
	1994/95 %	**1995/96 %**	**1996/97 %**	**1997/98 %**	**1998/99 %**	**1999/00 %**
Private Sector	41	49	55	49	41	37
Public Sector	59	51	45	51	59	63

Many access complaints are resolved after further information has been made available. Of the complaints received this year, 48% involve an access review. This includes access to personal health information under the Health Information Privacy Code and requests for information under section 22F of the Health Act 1956.

Some typical complaints about access from this year are as follows:

- A complainant became aware that a government agency had conducted an investigation about her. She requested access to the information held about the investigation and its outcome. She was advised that no information was held about the investigation and she was advised of the outcome. Enquiries were made with the agency concerned who advised that the investigation was carried out by its staff and any notes made had been destroyed before the request was made. The agency was asked whether the person carrying out the investigation could recall any aspects of the investigation. The person who carried out the investigation then wrote a summary of the enquiries made during the investigation and a summary was made available, which satisfied the complainant.

- Under section 22F of the Health Act 1956, individuals and their representatives are able to request information held by a health agency about that individual. The term "representative" is defined in part as meaning, where the individual is dead, that individual's "personal representative". This is a legal term referring to the deceased person's executor or administrator. A doctor received a request for access to a deceased woman's medical records. The request was made by the deceased woman's husband through his daughter, who was acting as her father's agent. The doctor refused the request and enquiries established that the deceased woman had no executor or administrator because she had no estate at the time of her death. The doctor concerned advised me that while the woman was alive, she refused to allow the doctor to disclose her medical records to her family. The doctor was of the view that she would not have wanted this to occur, even after her death. I formed the opinion that the husband was not his wife's personal representative and therefore was not entitled to access to the information under section 22F of the Health Act.

Complaints involving disclosure

These complaints involve allegations of disclosure contrary to information privacy principle 11 or rule 11 of the Health Information Privacy Code. Disclosure complaints form the second largest group of complaints.

TABLE 3: COMPLAINTS INVOLVING DISCLOSURE BY SECTOR 1995-2000						
	1994/95 %	1995/96 %	1996/97 %	1997/98 %	1998/99 %	1999/00 %
Private	67	71	73	65	59	61
Public	33	29	27	25	41	39
	1994/95	**1995/96**	**1996/97**	**1997/98**	**1998/99**	**1999/00**
Private	206	250	271	195	186	161
Public	103	102	100	105	130	103
Total	**309**	**352**	**371**	**300**	**316**	**264**

Figures for disclosure complaints are taken from those complaints that are closed within jurisdiction and involve disclosure. Complaints may also involve breaches of other principles as well as principle 11.

Some typical complaints about disclosure from this year are as follows:

- The complainant was a patient at a pain clinic. He was being treated for depression and had in the past expressed suicidal thoughts. The complainant failed to attend an appointment at the clinic but rang and left a message with the doctor that the reason he had not attended was that he had been purchasing a gun. The doctor rang the complainant the following day and the complainant decided to withdraw from treatment at the pain clinic. The doctor then consulted with colleagues, the local mental health community centre and the complainant's GP. The doctor decided to contact the Police and express his concern for the complainant's safety due to his depression and the purchase of the gun. I formed the opinion that the hospital could rely on an exception to rule 11 (which limits the disclosure of health information) on the grounds that the disclosure was necessary in order to prevent or lessen a serious and imminent threat to the complainant and his immediate family.

- The complainant received a letter from the Department of Corrections and on the back of the letter was a return address, including the words "Community Probation Service." The complainant considered that displaying this information disclosed information about him to any one else who may have seen the envelope. There was no evidence to suggest that anyone had seen the envelope in this particular case and therefore an interference with privacy could not be substantiated. The Department considered it was important to have a return address showing the name of the Probation Service as this alerted the recipient to the fact that the envelope contained important information and also increased the likelihood that letters wrongly addressed would be returned. However, the Department agreed to remove the words "Community Probation Service" from further envelopes and to just retain the name of the Department and the PO Box number. I considered this to be a useful outcome as large government departments correspond with people for a number of reasons and receiving a letter from such a department would not necessarily disclose anything adverse about the recipient.

Alleged breaches

Although access to information and disclosure of information form the two largest areas for complaints, complaints were received about alleged breaches of the other principles, with the exception of principle 12 which deals with unique identifiers.

Table 4 lists all alleged breaches. Some complaints allege a breach of more than one principle so the total exceeds the total of complaints received.

Examples of complaints involving breaches, other than access or disclosure included:

- Under Principle 7 of the Act an individual is able to make a request to an agency for correction of information it holds. Principle 7 also obliges an agency to ensure that, having regard to the purposes for which the information may be used, the information it holds is accurate, up-to-date, complete and not misleading. When an agency corrects information it holds the agency is obliged, where practicable, to inform each agency to whom the personal information has been disclosed of the steps it took to correct the information. I received a complaint that a government agency had notified a debt collection agency of a debt allegedly owed by the

TABLE 4: ALLEGED BREACHES 1999/00		
Alleged Breach	**Total**	**Percentage**
Information Privace Principle (IPP) 1 - Purpose	50	5.2
IPP 2 - Source	29	3.0
IPP 3 - Collection	26	2.7
IPP 4 - Manner	22	2.3
IPP 5 - Stroage	37	3.9
IPP 6 - Access	307	32.1
IPP 7 - Correction	23	2.4
IPP 8 - Accuracy	63	6.6
IPP 9 - Retention	7	0.7
IPP10 - Use	7	0.7
IPP 11 - Disclosure	199	20.8
Public Register Privacy Principle 2	2	0.2
Public Register Privacy Principle 3	1	0.1
Information Matching	1	0.1
Health Information Privacy Code (HIPC) Rule 1	4	0.4
HIPC Rule 3	5	0.5
HIPC Rule 4	2	0.2
HIPC Rule 5	14	1.5
HIPC Rule 6	62	6.5
HIPC Rule 7	4	0.4
HIPC Rule 8	6	0.6
HIPC Rule 10	4	0.4
HIPC Rule 11	65	0.7
Health Act, section 22F	14	1.5
HIPC Clause 6 - charges	1	0.1
N/A	1	0.1
Total	956	

complainant. The complainant exercised her statutory right of review of the debt, but the agency did not advise the debt collection agency that the default was in dispute and that further collection action should not be taken. The complainant ended up with a judgment against her which was published in the *Mercantile Gazette* and entered on her credit history. She was also summonsed to appear in court. After further investigation the agency disestablished the debt and the judgments were removed.

- The complainants went to a private house where an individual operated a photographic agency. The two women were shown to a changing area to change clothes for the photography session. They became aware that a video recorder was hidden among items on a shelf. As evidence of this surreptitious recording they took a video tape which was lying nearby and handed it to the Police. On that tape were recordings of the two women from a previous session. I considered that the action in secretly videoing the two women getting undressed was in breach of principle 4 of the Privacy Act which deals with the manner of collection of personal information. The photographer agreed to pay the complainants $8,500 but as he could not afford the amount in full, an arrangement was made to make periodic payments which are continuing.

Organisation type

Table 5 shows the types of organisations about which I have received complaints and the total complaints against each organisation. Not surprisingly, the government is the organisational grouping with the largest number of complaints made against it. It includes such agencies as the New Zealand Police, Department of Work and Income and Accident Compensation Corporation. The health sector is the next largest grouping and this includes hospitals, medical centres (including GPs) and a "catch all" category of "other" which includes agencies such as physiotherapists, dentists and specialists. The third largest category is "other business" which includes all those agencies such as retail shops, factories and finance companies which do not have a specific category in the list.

Top 8 respondents

I have listed the top eight respondents as on this years statistics there are only eight agencies which show more than a handful of complaints for the year. They attracted one third of the total complaints received for the year. However, it should not be assumed that the agencies listed are lacking in their Privacy Act compliance. Some agencies will, by the very nature of their dealings with the public and the sensitive nature of the information they hold, be subject to more complaints than other agencies.

An exception is New Zealand Police which I believe often takes a defensive position and is the only government agency I have had to refer to the Proceedings Commissioner. Proceedings brought have

TABLE 5: ORGANISATION TYPES 1999/00		
Government	276	34.54
Other (Business)	125	15.64
Health (Other)	107	13.39
Education	37	4.63
Local Authority	28	3.50
Hospital	27	3.38
Banking	25	3.13
Law Firm	25	3.13
Insurance	20	2.50
Telecommunications	17	2.13
Debt Collection Agency	15	1.88
Medical Centre (GP)	14	1.75
Club	9	1.13
Credit Reporting Agency	9	1.13
Individual	9	1.13
Courts	8	1.00
Real Estate	7	0.88
Voluntary Organisations	7	0.88
Religious Organisations	5	0.63
Trust	5	0.63
Direct Marketing	4	0.50
Industry Association	4	0.50
Media	3	0.38
Incorporated Societies	2	0.25
Landlord/Tenant	2	0.25
Licensing Trust	2	0.25
Trade Union	2	0.25
Accountant	1	0.13
Casino	1	0.13
Personnel Agency	1	0.13
Private Investigator	1	0.13
Total	**798**	

been successful. I have gained the clear impression that those dealing with complaints are under-resourced and this may lead to a complete denial approach to cases where I have later found the complaint has substance. That said, such cases are a minority of the complaints lodged against the Police. In respect of access requests, the Police seem to be guilty of undue delay in too many cases. I have taken up the issue of Privacy Act and Official Information Act training and inadequate policies, so far without tangible result. I will continue to pursue these matters.

The complaints included in this table comprise the complaints made against these agencies in the 1999/2000 financial year.

TABLE 6: TOP 8 RESPONDENTS 1999/00	
Agency	**Number of Complaints**
Department of Work and Income	62
NZ Police	56
Accident Compensation Corporation	44
Department of Corrections	27
Department of Child, Youth and Family	22
IRD	20
Telecom NZ Ltd	14
Baycorp Holdings Ltd*	11
* Includes Baynet CRA Ltd and Bay Collection Ltd	

Complaints Review Tribunal

If my staff have not brought about a settlement, I may refer complaints which in my opinion have substance to the Proceed-

TABLE 7: COMPLAINANT REFERRALS OUTCOME 1999/00	
Struck out	12
Proceedings dismissed	1
Breach	2
Withdrawn	3
Settled	1
Pending	8
Total	**27**

ings Commissioner with a view to instituting proceedings before the Complaints Review Tribunal. If I decide not to do this, I tell complainants of their right to take their own proceedings in the Complaints Review Tribunal. Also complainants whose complaints were not upheld can commence proceedings before the Tribunal.

Twenty-seven cases were taken by complainants to the Tribunal.

I referred four complaints to the Proceedings Commissioner. These four cases are pending. Four cases referred to the Proceedings Commissioner before 1 July 1999 were resolved.

TABLE 8: OUTCOME OF PRIOR REFERRALS

1.	**Breach of principle 6**	$200 damages	Complaints Review Tribunal
2.	**Breach of principle 6**	$8,000 damages $5,500 costs	High Court on appeal
3.	**No of breach of principles 3 and 4**		Court of Appeal on appeal from High Court
4.	**Breach of principle 11**	$10,000 damages	Complaints Review Tribunal

EDUCATION AND PUBLICITY

Seminars, conferences and workshops

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

Two kinds of workshops are offered. Standard workshops are offered on a regular basis during the year. These include half-day introductions to both the Privacy Act and Health Information Privacy Code and a full day workshop aimed specifically at the mental health sector. Twenty-two of these workshops were offered in Auckland and Wellington. Some of the standard workshops were provided to organisations that had a number of staff wishing to attend.

I also offer tailored workshops, designed as introductions to the Privacy Act or Health Information Privacy Code, but specifically adapted to the organisation involved. Agencies such as hospitals find this type of workshop useful as it enables the agency to train a number of staff at a time and also ensures that the training is relevant to the work carried out by the agency.

The workshops have been very successful in terms of participant satisfaction. My staff consistently receive very good or excellent evaluations and the workshops consistently meet participants' expectations. Training carried out in the workplace enables my staff to meet with frontline staff who are required to deal with Privacy Act requests or to make decisions on disclosures and this has increased our rapport with outside agencies and has increased understanding on both sides.

Two one-day Privacy Forums, planned during the year were held in Wellington and Auckland shortly after the end of the reporting period.

Printed resources

The first edition of *On the Record: A Practical Guide to Health Information Privacy* was published in October 1999. It was developed as a user-friendly guide to health information privacy issues. Case examples are provided throughout. Feedback from a number of agencies is that they have found *On the Record* to be useful as a quick reference point when dealing with health information privacy issues. A second edition was published in July 2000.

A new edition of the Health Information Privacy code 1994 was published in June 2000 and includes a revised explanatory commentary and new format and layout. All amendments to the Code to date are incorporated.

I continued my practice of releasing compilations of materials produced by my office. Two general compilations were released comprising papers, submissions and speeches.

During the year I released eleven case notes on complaints I had investigated. The objective of the case notes is to report some of the opinions I have reached on complaints, or to illustrate the types of complaints I receive 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 that demonstrated a facet of the application of the Act that 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.

Privacy issues in the media

Certain privacy related topics generated a great deal of publicity and media interest throughout the year.

ACC's request that medical professionals place coloured dots on the files of patients that they believe to be dangerous provoked intense media attention. The proposed ACC system for identifying instances of possible child abuse through repeat injury claims has also caused a great deal of debate and discussion.

Use of hidden cameras or covert surveillance is a widely held concern that was brought into sharp focus with allegations that cameras had been installed in the toilet cubicles of a South Island sawmill.

The Internet and e-commerce continue to be the source of a wide variety of information security and privacy concerns along

with similar developments in e-government. These and other technological issues receive regular coverage in the media.

Health information privacy is an ongoing area of public interest. There have been a number of incorrect and misleading statements by coroners indicating that the Privacy Act has prevented families from receiving information about deceased relatives.

Issues arising from the Gisborne cervical cancer inquiry brought close scrutiny of the scope of section 74 of the Health Act and the health information privacy rules.

Newsletter

Private Word, the newsletter, is an effective forum to discuss privacy issues and publicise the activities of the office. It continues to prove a popular way for agencies and individuals to keep up-to-date with privacy concerns and developments. The average print run has increased to 5,500 copies. During the year five issues were released including one double issue.

Current and past issues of *Private Word* are available on my website. 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

I have two full time Enquiries Officers who answer written and telephone enquiries made to my office. Enquiries are made by individuals seeking information about their entitlements under the Act, for example, whether or not they are allowed access to information about them held by their employer. I also receive enquiries from agencies collecting or holding information seeking clarification of their obligations under the Act.

Enquiries staff are sometimes the first contact point for individuals wishing to make a complaint to my office. Enquirers are given information about the relevant provisions of the Privacy Act and are given an indication of the information that is required by my office in order to commence an investigation. If the individuals have not already approached the agency concerned, they are encouraged to do so as the agency's privacy officer may be able to deal with the matter quickly and informally.

Enquiries received

TABLE 9: ENQUIRIES 1995-2000

	1995/96	1996/97	1997/98	1998/99	1999/00
Telephone	*	8,440	10,606	6,356	5,232
Written	*	595	535	615	571
Total	10,200	9,035	11,141	6,971	5,803
Av. per month	850	753	928	580	484

*** figures not available**

The number of enquiries received has fallen for the second year in a row. During the financial year 1998/99 I reduced the number of enquiry officers from three to two due to funding constraints. I have a free 0800 telephone number for enquiries but, due to the reduction of staff, many of the telephone enquiries are diverted to an answerphone system. We attempt to return those calls the same day but the answerphone system may account for the reduction in telephone enquiries. We received an increasing proportion of enquiries by e-mail which are included in the statistics for written enquiries. I received 5,232 telephone enquiries last year and 571 written enquiries. A total of 5,803 enquiries were received in the last year, with an average of 484 enquiries per month. All the enquiries received last year were dealt with by the end of July 2000.

Where we have received an answerphone message, three attempts are made to contact the person, but if this is unsuccessful no further action is taken. Our answerphone message alerts people to the existence of our website and some enquirers are able to obtain the information required from that site without further assistance from the office.

Enquiry topics

The new driver licence regime continued to generate a number of enquiries. Most of these enquirers were concerned with the requirement to have their photograph and signature stored digitally.

Another theme that carried on from previous years were enquiries about mailing lists. Enquirers were concerned about how direct marketers had obtained their details and requested information about how to get off mailing lists.

We also received a number of enquiries from individuals whose employers or prospective employers required them to authorise access to criminal conviction lists held either by the Department for Courts or the New Zealand Police. In some cases applicants for employment were required to provide authorisation to access criminal conviction histories and were required to answer extensive medical questionnaires. Many enquirers felt that the collection of such information at the application stage (as opposed to shortlist or appointment stage) was unnecessarily intrusive.

The health sector generated the greatest number of enquiries and the majority of these enquiries dealt with access to information and disclosure of information.

The Penal Institution Regulations 1999 also generated a number of enquiries. Clause 79 of those regulations requires most prison visitors to provide the following information:

- the visitor's date of birth;
- the inmate's name;
- the nature of the visitor's relationship with the inmate (if any);
- whether the visitor has ever served a sentence of imprisonment, and if so when;

- whether the visitor is currently on bail;
- whether the visitor has been convicted of an offence within the last two years;
- whether the visitor has ever been refused admittance to the institution or any other institution, as a visitor.

Many of the enquirers considered this collection of information to be unnecessarily intrusive.

Website

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 the office newsletter *Private Word* are all available on the website. Many written enquiries are also received and returned by e-mail. Fact sheets and other information can be attached to such responses.

My enquiries staff, along with the investigating officers, are also involved in the education function of the office.

SECTION 54 AUTHORISATIONS

This provision is important because it allows me to authorise actions that might otherwise be a breach of principles 2, 10 or 11. It can be useful when some disclosure ought to be made in the public interest where there is a duty under the Act not to disclose, perhaps because of a failure on the agency's part to provide for all eventualities. It allows for an unanticipated collection, use or disclosure that is in the public interest or in the interests of the person concerned. It exists as a "safety valve" to address rare and unexpected problems.

In considering applications, I evaluate whether in the special circumstances of the case, any interference with the privacy of an individual that could result from the action in question is substantially outweighed by either the:

- public interest in that action; or
- clear benefit to the individual concerned.

Detailed guidelines for any agency considering applying for an authorisation are available at my website (www.privacy.org.nz) or upon request from my office.

One application for an authorisation was carried over from last year, with four new applications received this year. I declined three applications.

One of the applications was declined because it appeared that the information the applicant sought to disclose was sourced from a public register. There was no need for the exemption.

Another applicant requested that I authorise the disclosure of third party current address details from a government agency. The agency had refused to disclose the information to the applicant. I do not consider it appropriate to grant an authorisation when the agency holding the information is unwilling to release it. An authorisation does not require an agency to disclose information and I have no power to order a disclosure.

A further application was declined because the agency making the application was not the agency intending to disclose information. It was not confirmed that the agencies holding the information were willing for it to be disclosed.

Two of the five applications remained under consideration at the end of the year. One of these has subsequently been granted. No exemptions were granted in the reporting period.

LEGISLATION

One of my roles is to act as a "privacy watchdog" in relation to new laws. Legislation has a significant potential to impact on the privacy of individuals - frequently detrimental in effect, occasionally beneficial. Scrutiny of proposed new laws is especially important since, once passed, other statutes and regulations concerned with personal information will prevail over the information privacy principles in the Privacy Act.

The Cabinet Office Manual requires ministers to signify compliance with the principles and guidelines of the Privacy Act when seeking the introduction of bills into Parliament or when proposing the issue of regulations. Accordingly, I am frequently consulted by departments concerning new proposals.

My office also tries to scrutinise all bills introduced into Parliament. Where there are privacy implications my office is frequently consulted in the pre-introduction phase. However, that is not always the case. Sometimes privacy issues have not been recognised in advance by departments. Also, members' bills, introduced by government and opposition backbenchers have not usually been the subject of consultation. I am willing to comment on draft members' bills, if asked.

One of my functions is to examine any proposed legislation that may affect the privacy of individuals and to report to the Minister of Justice. During the year I submitted six reports to the Minister on proposed new legislation and a further supplementary report on my review of the operation of the Privacy Act. I record a selection of the legislative matters upon which I commented during the year.

Acts and Regulations Publication Amendment Bill

This bill was intended to confer power to publish reprints of Acts and statutory regulations in a modern format and style. I firmly support modernisation of the appearance and usability of New Zealand laws: I earlier adopted a more modern style, consistent with Law Commission recommendations, in the codes of practice issued under the Privacy Act. Following my detailed review of the operation of the Privacy Act (which included public consultation) I became convinced that the old fashioned style and layout of New Zealand statutes, including the Privacy Act, hindered understanding by members of the public.

The bill would mean, for instance, that when the Privacy Act is reprinted, the layout would be modernised in setting out the text of provisions, the positioning of section headings and modern use of capital and lower case letters. Changes to the text would also be allowed by omitting referential words (for example, "of this Act", "of this section" and "of this paragraph"). This would eliminate the scores, if not hundreds, of such phrases in the Privacy Act.

In my submission I made several suggestions regarding matters that did not appear to be addressed by the bill. Those touched upon the numbering of schedules, alternatives for "shall", the inclusion of material in the table of contents (or "analysis"), marginal notes, section notes and end notes. I also submitted that care would need to be taken in the presentation of the substituted material to avoid reprinted Acts highlighting the changes in a cluttered and unattractive manner. The select committee adopted one of my suggestions and took the view that several of the others were able to be addressed administratively in reprints without the need for explicit statutory authority.

Individually the changes made to statutes and reprints appear minor and have no substantive legal effect. However, cumulatively the changes represent an important modernisation of the New Zealand statute book. While the effect of the individual changes may be almost imperceptible to some, collectively they will make consulting a statute a less daunting task for non-legally trained people. This will bring benefits to users of the Privacy Act given that it is a law of wide application which is consulted by many non-lawyers.

Adoption Law Reform

In October 1999 the Law Commission released a discussion paper on options for reform of adoption law. This provided a good opportunity to look at the "big picture" in respect of some of the information privacy issues, particularly those touching on access to information. I contributed to the process by meeting with the Commission and making two submissions. The first submission touched briefly on a variety of privacy issues surrounding the adoption process such as the question of who may adopt, adoption orders, forbidden marriage and incest, cultural adoption practices and surrogacy. However, my major submission focused on access to adoption information.

Legislation bearing upon access to adoption information includes:

- Adoption Act 1955;
- Archives Act 1957;
- Official Information Act 1982;
- Adult Adoption Information Act 1985;
- Privacy Act 1993;
- Births, Deaths, and Marriages Registration Act 1995;
- Adoption (Intercountry) Act 1997.

The approach of, and philosophy underlying these enactments differ significantly in their treatment of adoption information. Reform could provide a consistent approach, offer humane solutions to currently vexing issues, and establish mechanisms to ensure that any new policy is effectively applied.

In the detailed submission I canvassed a suggested approach to law reform and addressed specific issues raised in the discussion paper concerning such matters as birth certificates, artificial reproductive technology, location of statutory rights, age restrictions on access, access entitlements of family members, and the merits of non-contact vetoes over information vetoes. Some of the opinions offered were tentatively expressed since there are such a range of options for reform and a host of philosophical, legal and practical issues to be gone into. The Law Commission had not reported by the end of the year but given the centrality of privacy and personal access issues, I expect that I will be consulted further on the issues by the Ministry of Justice as reform proceeds.

Business Law Reform Bill

This bill would amend the Financial Reporting Act 1993 so that the disclosure of personal information would not be a breach of information privacy principles 10 or 11 of the Privacy Act if required by an applicable financial reporting standard (FRS) that was approved after this bill is in force. An associated amendment to the Financial Reporting Act would mean that the Accounting Stand-

ards Review Board (ASRB) must not approve an FRS that is likely to require the disclosure of personal information unless the ASRB is satisfied that the Privacy Commissioner has been consulted.

The bill will give an FRS greater legal status than similarly placed delegated legislation which is not issued by Order in Council. I took the view that so long as ASRB processes could be structured so that privacy issues are identified before the issue of an FRS, and that those issues were considered carefully and where appropriate I was consulted, it would be appropriate to allow obligations in an FRS to override those obligations owed by an agency under principle 11. The amendment would resolve a dilemma into which agencies might be placed whereby one legal duty required them to comply with principle 11 while their duty under an applicable FRS required certain details to be disclosed in published accounts. I should add that for the most part it is not anticipated that disclosure of personal information about identifiable individuals would be required under any FRS. However, there might be circumstances in which the identity of an individual might be deduced from information published in accounts. The main cases anticipated where obligations might be imposed concern related-party transactions and itemised remuneration or expenditure disclosures.

My position was not to oppose the enactment of the provision concerning disclosure of information so long as the ASRB was required to consult. The bill remained before a select committee at the end of the period.

Coroners Act

During the year the Law Commission reviewed the Coroners Act. The Law Commission made a number of recommendations along the lines suggested in a submission made by my office touching upon, among other matters:

- suppression of evidence at public hearings;

- complaints against coroners who fail to accord the statutory rights to notify affected people in advance of adverse findings to individuals;

- extension of the rights of notification, access and the opportunity to be heard to same sex partners as with other immediate family and relatives;

- public access in the period after an inquest, to sensitive medical and other records presented in evidence.

The Law Commission's recommendations, if adopted, have the potential to enhance the protection of privacy in comparatively unusual and stressful circumstances. For example, the present law allows all manner of medical records to be made available for inspection by any person when an inquest has been held, whereas similar records would remain strictly confidential if the person died of natural causes. Release of certain sensitive details in open court, without controls on publication, can be highly embarrassing for family members without necessarily serving a particular public interest.

The review was also timely from my perspective since there had been comments made by several coroners as to constraints on disclosure of personal information attributed to the Privacy Act. Some of the comments were not, in my opinion, well informed as to the correct legal position and I have made some efforts to clarify the situation on particular occasions with the coroners involved. This has not always been successful and the Law Commission's proposal for the establishment of a Chief Coroner holds promise in terms of training on such issues. I therefore welcomed the opportunity at the end of the year when I was asked by the Auckland Coroner to prepare evidence on the legal position under the Health Information Privacy Code in terms of certain disclosures of mental health information.

Crimes Amendment Bill (No 6)

Commentators have suggested for many years that New Zealand's criminal laws are inadequate in so far as they relate to computer "hacking". In the early 1990s, the Crimes Consultative Committee recommended criminalising the accessing of computers for dishonest purposes, and damaging or interfering with computers. Since then the growth of the Internet and electronic commerce have made the issues even more pressing. In my review of the operation of the Privacy Act in 1998, I examined the issue as it affected individual privacy and in my report urged the government to enact offence provisions such as those recommended earlier.

In 1999 the Crimes Amendment Bill (No 6) proposed to insert new offence provisions into the Crimes Act 1961 concerning:

- accessing a computer system for a dishonest purpose; and

- damaging or interfering with computer systems.

I supported both such provisions. Although they were not directed toward protecting personal information, the deterrent effect might incidentally help protect privacy in the operation of computer databases. However, the law reform is not complete and the previous government had announced its intention to introduce a further provision outlawing the unauthorised access to a computer system regardless of whether any property damage is done or the offender has a dishonest purpose.

The new government also supported the enactment of such a provision. Policy work was undertaken during the year, in respect of which I was consulted, but the provision had not been introduced into Parliament by year's end. It is apparent that while an anti-hacking offence itself is uncontroversial, the creation of a statutory exemption for law enforcement and intelligence agencies will be. There is concern that the provision might become an open-ended authorisation for new electronic state surveillance. I will follow the matter closely during the coming year.

Evidence Code

In August 1999 the Law Commission submitted its major report on reform of the law of evidence. In a small way my office contributed to this project offering submissions on the following discussion papers released by the Law Commission:

- Evidence Law: Privilege (Preliminary Paper 23) - January 1995;
- Privilege against Self Incrimination (PP 25) - January 1997;
- Evidence of Children and other Vulnerable Witnesses (PP 26) - February 1997;
- Evidence Law: Character and Credibility (PP 27) - April 1997;
- Criminal Prosecution (PP 28) - April 1997.

During the period I also provided a report to the Justice and Law Reform Committee in relation to the Evidence (Witness Anonymity) Amendment Bill.

The Law Commission's report is the first stage of reform which will also involve further review at departmental, governmental and parliamentary levels. I will follow these matters with some interest given the effects on the privacy of individuals. As these processes can take some time, I have already suggested to the Minister of Justice that an aspect of the draft Evidence Code, concerning the right of witnesses to have a support person present with them in court should be taken forward in the Victims' Rights Bill (noted below).

Fisheries Amendment Bill

The Ministry of Fisheries manages a number of databases covering information on: fisheries resources, operation of fishing quotas, permits, catch reporting, enforcement of fisheries law, prosecution of offenders, and administration of fisheries business.

As part of MAF information management practices, a common client identifier is assigned. The identifier is used to identify persons involved in commercial fishing activities within the various collections for policy analysis, law enforcement, allocation of special permit and reporting purposes. There is no particular compliance problem with information privacy principle 12 in the Ministry using a unique identifier in these circumstances.

However, the Fisheries Amendment Bill anticipated that some fisheries services activities will be devolved to private sector companies to undertake on behalf of MAF. It was anticipated that these approved service delivery organisations (ASDOs) would need to utilise the same unique identifier as the Ministry. This would contravene information privacy principle 12.

The Department canvassed with my office the need for, and alternatives to, a shared unique identifier. Consideration was given to the possibility of a code of practice issued under the Privacy Act or statutory authorisation in the Fisheries Amendment Bill to exempt the practice from principle 12. After studying the documentation given to my office, I was persuaded of the merit in permitting the shared use of a common unique identifier. I believe that this should be authorised by the amendment bill rather than a code. I urged an approach which was proportionate to the business need for a common identifier and which controlled the use of those identifiers by ASDOs and others for unrelated purposes.

The resultant provision, later enacted into law, provided:

296ZH. Unique identifiers

(1) The purpose of this section is:

(a) to enable approved service delivery organisations to assign to any persons specified in section 189 unique identifiers that have been assigned by the Chief Executive; and

(b) to restrict approved service delivery organisations from using such unique identifiers for purposes other then carrying out the specified functions, duties, or powers transferred to them under section 296B.

(2) Despite information privacy principle 12(2) of the Privacy Act 1993 an approved service delivery organisation may assign to any person specified in section 189 any unique identifier assigned to that person by the chief executive.

(3) This section does not authorise an approved service delivery organisation to use a unique identifier assigned by the chief executive, except for the purpose of carrying out specified functions, duties, or powers that have been transferred to the approved service delivery organisation under section 296B.

I was satisfied with the approach finally taken. As with many such cases, the department worked through the issues in a co-operative and helpful way with my office. A solution was arrived at which meant that the business needs of the department, governmental objectives and protection compatible with the information privacy principles were all accommodated.

Privacy Act Review

In December 1998 I submitted my first report under section 26 of Privacy Act to the Rt Hon Sir Douglas Graham, then Minister of Justice, following a detailed review of the operation of the Act. *Necessary and Desirable: Privacy Act 1993 Review* had essentially been completed by June 1998 with the rest of that calendar year being devoted to checking details, final consultation and preparing the report for publication. A draft version of the report had been given to the Ministry of Justice in July 1998.

By 2000 the Ministry had done no detailed policy work in relation to the report and recommendations. Given the length of time that had elapsed I concluded that it would be useful to further reflect on aspects of the operation of the Act with a view to providing a supplementary report. I submitted this in April 2000. While my

focus in that report was mainly on issues not earlier identified, I also elaborated on some of the previous recommendations having considered matters further. I also highlighted cases where an earlier recommendation had been affected by subsequent events, such as where new legislation had been introduced since 1998.

The supplementary report, with its 16 recommendations was designed to fit with the original report and form a complementary package for policy makers to study at the appropriate time. I have urged that the matter be taken forward as there are a number of important matters contained in my recommendations ranging from fine tuning through to enhancing individuals' rights. Parliament itself required that such a review be undertaken and obviously the review cannot serve its intended useful purpose without being taken to the next stage.

Public Audit Bill

The Auditor-General, and his or her agents, has access to confidential information in the course of performing statutory functions. Resultant audit reports give assurance to the entities concerned, Parliament and the public about the use of public money and resources. The bill modernised the statutory basis on which the Auditor-General operates.

I was consulted by the Auditor-General about this bill before it was introduced. Of particular note was a change in powers to access bank account records. Under the 1977 Act the Auditor-General has powers to directly demand access to bank account details. In the bill, a district court warrant is required. This would not impede the effectiveness of the Auditor-General since such powers are used sparingly. The introduction of a warrant process will not only protect privacy but should also enhance public confidence in the exercise of such significant powers.

Tax Administration Act

In mid-1999 the Finance and Expenditure Committee (FEC) commenced an inquiry into the powers and operations of the Inland Revenue Department. The FEC invited me to make a submission as it was particularly interested in the matter of access by the individuals concerned to personal information held about them by IRD.

The right of individual access is important in a variety of ways. Lying behind privacy legislation is a recognition of an individual's entitlement to some degree of personal autonomy. That autonomy would be illusory in many cases unless the individual could see what information is held for potential use by others. Another reason for the right of access is the concern that personal information used should be accurate. Possibly the best way of ensuring such accuracy is to let the person concerned point out any errors. It provides some measure of accountability by agencies to the individual whose personal information they hold and may use. Finally, an individual's right of access tends to make other aspects of information privacy principles self-policing. Objectionable handling of personal information may come to light through the individual's access to it.

Section 81 of the Tax Administration Act 1994 obliges every officer of IRD to maintain secrecy with respect to all matters relating to the Inland Revenue Acts (including all statutes administered by the IRD) coming into the officer's knowledge. There are a number of specified exceptions to the secrecy required by section 81 allowing the use of tax information for important, but limited, purposes within government service. However, among numerous statutory exceptions of obligations of secrecy there is none saving individual rights of access under information privacy principle 6.

The existence of the secrecy provision means that the access rights under the Privacy Act are effectively ousted. People are free to request information but the IRD may quite properly rely upon section 81 to refuse requests. The Department may, in its discretion, nonetheless release information upon request where, for instance, it believes the disclosure carries into effect the Inland Revenue Acts. If the information is refused there is little that I can do under the Privacy Act, although the Commissioner of Inland Revenue might be persuaded in particular cases to give an individual access to information that was previously refused.

Obviously near-absolute confidentiality or secrecy is a basic tenet of the tax system and is fundamental to the trust that taxpayers place in dealings with IRD. The existence of the secrecy provision is important not only to require IRD to respect confidentiality but also to enable the Department to resist requests from other departments, authorities and individuals for the release of information it holds about taxpayers. I support the continuing existence of a strong secrecy provision.

I submitted to the FEC that section 81 should be amended to ensure that individuals *as of right* have access under information privacy principle 6 to information held about them by IRD. A right is quite different from the discretionary release of information. It ensures that the individual's hand is strengthened against a huge bureaucracy. Rights come with enforceable remedies. For example, damages can be obtained for undue delay or for the withholding of information with no proper basis.

I also raised with the FEC the potential problem of enforced subject access (sometimes called coerced access) where third parties compel individuals to exercise their access rights so as to release information to that third party. It would be desirable for IRD to release information only to the individual concerned, and not to third parties, and that coerced access be outlawed.

I was pleased to note that the FEC made a recommendation consistent with my suggestions and proposed that section 81 be amended to allow access pursuant to information privacy principle 6. The Committee declined to follow an alternative proposal that the right of access should be under the Official Information Act which would provide no remedy by way of damages. It also proposed that the matter of coerced access be addressed. On another matter that I had raised with the Committee, the FEC recommended that a form of electronic "footprinting" be established to address the dual problems of staff browsing taxpayer records and corrupt disclosure.

The recommendations had not been implemented by the end of the year but the Government had agreed to the personal access recommendation (subject to ensuring that access did not infringe on the privacy rights of other taxpayers or adversely affect collection of revenue) and agreed with the general intent of the electronic footprinting recommendation. The former recommendation turns on legal and administrative issues while the latter also raises certain technical issues such as grafting footprinting onto a system that presently has none. I will follow closely the IRD's and Government's response to the legal, administrative and technical issues.

Victims' Rights Bill

The unavoidable involvement of victims in the criminal justice system may sometimes add to their trauma and hardship. The Victims of Offences Act 1987 sought to minimise this by giving effect

to the UN Declaration of Basic Principles of Justice for Victims of Crimes and Abuse of Power.

I examined this bill which would replace the 1987 Act as it would affect the privacy of individuals. Victims may sometimes be deterred from reporting crimes or co-operating with investigations without suitable protections, including to their privacy. The bill has the potential to better protect the privacy of victims than is currently the case.

In December 1999 I submitted a report to the Minister of Justice. I supported provisions to place better controls on the dissemination of copies of victim impact statements (which reportedly have been passed hand to hand around prisons). I also commented on provisions that will sometimes enable caregivers to receive notifications of an impending prison release instead of victims being notified personally.

Amongst a variety of other suggestions, I recommended that:

- the Evidence Act 1908 be amended to strengthen the protections governing the privacy of a witness's precise address in court;

- my earlier recommendations be acted upon to enable suppression of details on public registers where individuals have personal safety or harassment fears (which could include in this context victims, witnesses, jury members, law enforcement officials, and judicial officers);

- consideration be given to enabling notifications from the victim notification register to be given electronically;

- victims be entitled to have a support person present in criminal proceedings.

The bill remained before a select committee at the end of the reporting period. The new Government had announced its intention to introduce further major amendments. They too are likely to have privacy implications and I will study them carefully.

INTERNATIONAL DIMENSION

There is quite an international dimension to work in the field of information privacy and data protection. Consider, for example:

International instruments: New Zealand's information privacy principles were drafted to implement and be consistent with the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (1980). Twenty-nine of the world's industrialised democracies belong to the OECD and give effect to the guidelines in law or practice. The 15 member states of the European Union are subject to a Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data (1995), while a wider group of European countries are bound by similar provisions in the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (1981). Rights under the Convention and Directive are legally enforceable. At United Nations level, the General Assembly has adopted Guidelines for the Regulation of Computerised Personal Data Files (1990) and more recently, in the context of world trade, the General Agreement on Trade in Services (GATS, Article XIV) recognises the protection of personal data as a legitimate reason for blocking information flows and the free movement of services. Beyond the end of the reporting period I note that the proposed agreement with Singapore on a closer economic partnership recognises that information is not required to be disclosed in contravention of laws protecting personal privacy (Article 77).

Information and communication technology: Advances in information technology, allowing for the collection, storage, retrieval, linking, manipulation and use of vast amounts of information, together with advances in communications technology and management, have truly established today's "information society" or "global information infrastructure". New technologies, the application of existing technologies to new tasks, and the convergence of technologies, continues apace and the phenomenon is global. Technological developments in Tokyo or San Francisco directly affect New Zealand citizens and responses to data protection issues cannot always be devised in New Zealand without looking beyond our borders. My work has been informed by analysis undertaken and responses developed by colleagues in similar offices overseas and by other organisa-

tions such as public advocacy groups, telecommunications regulators, academics, technical experts and legislators. (Conversely, there has been keen interest in Canada and Australia in the New Zealand law: particularly our approach of treating public and private sectors alike, our responses to public register issues and the ability to modify the general law by code of practice.)

Variations in levels of data protection: There remains a disparity in levels of protection of privacy throughout the world. The norm within developed countries of our type can now be said to consist of a national law based on international principles, similar to the Privacy Act, with a national supervisory body, similar to the Privacy Commissioner, having a key role to ensure that the law is effective. One exception which has attracted considerable attention is the USA. However, even the USA has a federal Privacy Act and many sectoral privacy laws covering parts of the private sector. Such laws are consistent with the OECD Guidelines and indeed many of them offer exceptionally strong data protection. Of course, the picture differs in the developing world and most of our Pacific Island and Asian neighbours do not offer adequate data protection in law. Given the global economy, electronic commerce and transborder data flows, the absence of such protections is not a matter simply of national interest but attracts international attention as well. In particular, the European Union, one of the world's major trading blocs, is in the process of judging whether each country offers "adequate data protection" and prohibiting the export of personal data to jurisdictions which do not.

Regional and international cooperation

The international links, and cooperative arrangements, with similarly placed privacy and data protection commissioners overseas continues to be of value to my work. This period saw a considerable amount of international activity in our region.

At the trans-Tasman level, the Privacy Agencies of New Zealand and Australia (PANZA) met in Sydney. Australia is paying increasing attention to the protection of privacy in the private sector. A set of national privacy principles, developed by the former Australian Privacy Commissioner at the request of the Prime Minister, have been incorporated into a number of industry self-regulatory codes and are to be implemented by law in the private sector by an extension of the Commonwealth Privacy Act. As well as issues such as this, the PANZA discussions in Sydney ranged through the forensic use of DNA,

sports drug testing, medical information, proof of identity, civil liability for invasion of privacy and a number of other matters.

At regional level I convened, with the Australian Privacy Commissioner, the Second Asia Pacific Forum on Privacy and Data Protection. The ASPAC II Forum was held in Hong Kong with representation from the following:

- Australia
- Canada
- Federated States of Micronesia
- Fiji
- Hawaii
- Hong Kong
- India
- Indonesia
- Malaysia
- New Zealand
- Papua New Guinea
- Samoa
- Solomon Islands
- Thailand
- The Philippines
- Tonga
- Tuvalu.

Participation from Pacific Island states was only possible through the support of the New Zealand Ministry of Foreign Affairs and Trade's Good Governance Fund. The Forum received jurisdiction reports from a variety of legal systems and countries ranging from the tiny to the huge. Presentations were given by experts from Europe, North America and our own region promoting discussion on:

- readily available privacy and data protection resources in published form and on the Internet;
- data export issues;
- comparative models of national data protection agencies;
- the ability of agencies to confront systematic data protection issues;
- a case study in adaptation of privacy principles.

I followed up this work with Pacific countries with a paper "Legal Challenges for Small Jurisdictions" at a meeting of bar leaders of 16 Pacific nations held in Nadi, Fiji in January this year. The meeting had been arranged and financed by the International Bar Association's General Professional Purposes Committee to engage and assist the small numbers of lawyers confronting complex legal issues to bring themselves up-to-date with international trends and changes.

I believe it will be necessary to develop a model privacy law for small jurisdictions if they are not to suffer in the international business arena. I was at the end of the year exploring possibilities for such an initiative.

The Asia Pacific Forum preceded the 21st International Conference of Privacy and Data Protection Commissioners which was hosted by the Hong Kong Privacy Commissioner for Personal Data. This is the premier data protection and privacy conference and brings together data protection regulators and privacy experts from throughout the world. Among the sessions, I and the Assistant Commissioner, contributed to a panel addressing public register privacy problems and solutions.

Associated with the International Conference and the ASPAC II Forum, my office arranged two other meetings in Hong Kong. The first was a briefing for those Asian and Pacific Island delegates who were new to the subject. The second was a practical skills workshop for Commissioners and staff on developing websites and dealing with problem complainants. This workshop attracted participation from Australia, Canada, Hong Kong, Hungary, Jersey, the UK and Hawaii and continued a series of practical skills workshops I had convened at earlier commissioners' conferences.

Finally, in association with the work being undertaken on a code of practice on telecommunications, the Assistant Commissioner participated in a meeting of the International Working Group on Data Protection in Telecommunications. This is a specialist group established by the international conference to undertake ongoing research into privacy issues in telecommunications, the Internet and the media. The common positions that have been developed by this working group over the years offer valuable guidance on specialist issues and I have made a consolidated reprint of them available in New Zealand.

Electronic commerce and websites

No one can fail to be impressed by how the burgeoning Internet, and the related technologies brought together under the rubric of electronic commerce, have entered so many areas of business, government and leisure. While growth may look set to continue for some time, the speed of take-up of electronic commerce will depend in part on consumer and citizen confidence in the technology and in the way in which personal information is respected and

handled in transactions. There is considerable evidence that fair information practices and effective privacy rights are keys to successful e-commerce.

In the area of "business to consumer" (or "B2C" in the jargon) transactions, enforceable rules and remedies, such as those provided through the Privacy Act, are essential. Equally important is good practice by the host of businesses with whom consumers deal. At its most basic, and consistent with information privacy principle 3, businesses with a presence on the web must state what their privacy policies are and stick to them. In other words, businesses must "say what you do and do what you say". Many New Zealand businesses do not yet include privacy statements as they ought to. I encourage consumers to take up the issue with businesses who do not display a website statement. Consumers should send them an email asking why a policy has not been posted. New Zealand government sites should also take a lead here given the emphasis the government wishes to place on e-government. I will be looking at the matter further in the new year.

Resolving issues about transborder data flows, which typically is a "business to business" (or B2B) issue, is also important to international e-commerce. If the European Union formally finds that the New Zealand Privacy Act offers an "adequate standard of data protection" this will give a degree of business "trust" to deal with New Zealand companies and offer our traders a comparative advantage in that area. I have encouraged this and the previous government to act to secure a positive EU finding. It would require two amendments to the Privacy Act to address the issues of data re-export and foreigners' access and correction rights. While no amendments were made to the Act during the year, the Law Commission in its *Electronic Commerce: Part Two* report endorsed my recommendations on this issue. I have been surprised that business lobby groups show little interest in pressing for this to occur - it may reflect a complacency or lethargy about competing in the international marketplace in other than traditional fields.

FUNCTIONS UNDER OTHER ENACTMENTS

A number of functions, powers and duties are conferred or imposed upon me by enactments other than the Privacy Act. The statutory provisions in question tend to be of four types:

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

It can be convenient for a government or for Parliament to confer functions on the Privacy Commissioner in another law for several reasons. For example, a proposal contained in that law might raise public concerns. Without abandoning the basic proposal, conferring a special "watchdog" role upon the Commissioner may allay public concern and allow the proposal to proceed. Typically, this might involve requiring a public agency to consult with the Privacy Commissioner in the implementation of a new scheme. A complaints role might be conferred upon the Commissioner in anticipation of exceptional circumstances if there is concern that new powers might be used in an unexpected or unreasonable way or that something might go wrong. Placing a complaints function with the Privacy Commissioner is cheaper than creating a special new procedure, or complaints body, especially when complaints are expected to arise only rarely.

Complaints under other legislation

Although comparatively few complaints were received under my alternative complaints jurisdictions, each fulfils an important check on the exercise of particular statutory powers. The mere existence of a right to complain about the effect on privacy from the exercise of another statutory function can lead to additional care being taken by officials in the exercise of their statutory powers - including developing 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 has been discussed in more detail in earlier annual reports. Fourteen complaints alleging refusal to provide health records under section 22F were received this year.

Part VI of the Domestic Violence Act 1995 gives me jurisdiction to investigate complaints against refusals by registrars to suppress residential details on certain public registers following an application from someone who has had a protection order and fears for his or her personal safety if those details were to be released. No complaints under the Domestic Violence Act were received this year.

Section 11B of the Social Security Act 1964 provides that a person may complain to the Privacy Commissioner about a breach of a code of conduct issued by the Director-General of Social Welfare under that section (now the Chief Executive of the Department of Work and Income). 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 Work and Income to supply information or documents about beneficiaries under section 11.

Approval of agreements

Section 35 of the Passports Act requires my approval to be obtained in relation to agreements to supply information from the passports database by the Department of Internal Affairs to the NZ Customs Service. My approval is also required for any changes to that agreement. No agreements have been approved to date, although during the year my office made comments on a draft agreement and, after a very lengthy process, it appears that a finalised agreement may be available in a satisfactory form to receive my approval in the next financial year.

Similarly, section 36 of the Passports Act requires my approval to be obtained in relation to agreements for the supply of information from the passports database to Australia. I have not approved any agreements or changes to any existing agreements during the year. The position since 1992 was set out in some length in my last annual report. Some progress was made during the year towards readying an agreement for my approval. However, progress is not as far advanced as with the agreement under section 35.

I regard as serious the fact that information from the passports database has been disclosed since 1992, and continues to be sup-

plied, in the absence of the approvals required by sections 35 and 36 of the Passports Act.

Consultations

The Official Information Act 1982 and the Local Government Official Information and Meetings Act 1987 require the Ombudsmen to consult with the Privacy Commissioner before forming a final view of official information access requests where privacy is a possible ground for withholding information. During the year 52 consultations under the two Acts were completed.

TABLE 10: CONSULTATIONS WITH THE OMBUDSMEN 1995-2000

Year	Number of consultations
1995/96	60
1996/97	87
1997/98	77
1998/99	66
1999/00	52

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 narrowly advocating a privacy viewpoint.

It is of concern to me that some public sector agencies, when faced with a request, consistently fail to deal with it in accordance with the Official Information Act and the Privacy Act. Rather than balancing the competing interests and making a careful assessment of the information to be released, some agencies simply withhold all or most of the file. Their analysis of the competing privacy and public interests can be rudimentary or, worse, non-existent. This trend is disturbing, given that access rights are not new. Agencies have had 17 years to become used to the regime imposed by the Official Information Act. One can only speculate that compliance might be taken more seriously if withholding information without reasonable grounds or undue delay could be met with awards of damages, as is possible with personal access requests under the Pri-

vacy Act. Entreaties by Ombudsmen in successive years do not seem to have had much effect – particularly on the habit of waiting 20 working days before responding to simple requests for a single document which is readily ascertainable.

At a practical level, this overly simplistic response has impacted on the workload of the Ombudsmen and my office. Rather than simply reviewing the decision, our staff have more to do by way of identifying the information at issue, and assessing and balancing the competing interests. I have only one staff member available to work part-time on consultations with the Ombudsmen, so this trend has affected my ability to respond in a timely fashion. This has also tended to encourage Ombudsmen to press for disclosure by way of provisional opinion, which is often acceded to prior to my consultation.

I have also noticed a growing disparity in the responses given by different branches of the same agency. Lack of consistency in approach is of some concern, and I have contacted some agencies to suggest privacy training would be in order.

I am often consulted in relation to so-called "golden handshakes" or severance payments. The majority of these requests relate to chief executive positions, but there have also been requests for information about senior managers. The Ombudsmen and my office have taken similar approaches to these requests.

I have taken the view that the public interest lies in knowledge of the extent of the cost to the employer of a payment rather than in the "dollars and cents" detail. The practice of offering a severance payment to certain departing senior public servants raises a number of issues and the reasons for the payments vary. The size of the payment is a relevant factor: there is little doubt that the public accountability for substantial payments or with payments that are disproportionate to the remuneration received militates in favour of disclosure.

While there may be a strong public interest in disclosure of the level of some severance payments, this is not always the case. Sometimes the payment is very modest or there may be family or medical reasons behind the departure and I have tended to give greater weight to the privacy of the individual in that information. The release of very specific payment details can be misleading as well as demeaning to the individual, particularly when there are

surrounding circumstances that put the payment in a different light but those circumstances are not widely known. Giving out some information can lead to demands for even more intrusive information to feed curiosity rather than accountability. A severance payment for the early termination of an employment contract may not indicate any inadequacy on the part of the employee, but often publicity is directed against the individual rather then the agency which has wanted to pay the sum involved. In a few cases confidentiality agreements are cited to resist an access request. When, at my suggestion, the employee is approached it is learned that it was the employer who sought and seeks to maintain the confidentiality while citing the privacy of the individual as the concern.

Appointment to other bodies

Under the Human Rights Act 1993 I am, by virtue of my appointment as Privacy Commissioner, also a Human Rights Commissioner. I attended eleven formal meetings of the Commission during the year.

I have been fulfilling the role of chairing the Commission since the end of the term of the previous Chief Human Rights Commissioner, Pamela Jeffries. This has demanded a significant additional time commitment at a time when the Associate Minister of Justice has undertaken a re-evaluation of human rights institutions.

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. Matching can be done manually with paper files but, as a practical matter, time and cost usually precludes this. The technique has particular attractions in detecting fraud in government programmes. The information matching with which I am principally concerned in relation to my functions under Part X of the Privacy Act relates to cases in which adverse action may be taken against individuals by public bodies.

Data matching is perceived to have negative effects on privacy by, amongst other things:

- 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 by someone;
- taking automated decisions affecting individuals without human intervention;
- requiring innocent people to prove their lack of guilt due to errors or wrong inferences arising from the matching process;
- multiplying the effects on individuals of errors in some government databases.

To address the risks, Part X of the Privacy Act authorises and regulates the practice of information matching. It does this through controls directed at:

- ***authorisation*** - ensuring that only programmes which appear to be well justified in the public interest are approved;

- ***operation*** - ensuring that programmes are operated consistently with fair information practices and that individuals are not "presumed guilty until they prove their innocence";

- ***evaluation*** - subjecting programmes to periodic reviews and possible discontinuance.

Operational controls and safeguards

Figure 2 illustrates something of the processes involved in authorised information matching programmes. The flowchart shown is simplified and generalised and so will not correspond to all authorised programmes. Nonetheless, it illustrates the typical stages and some of the safeguards to ensure fairness and data quality.

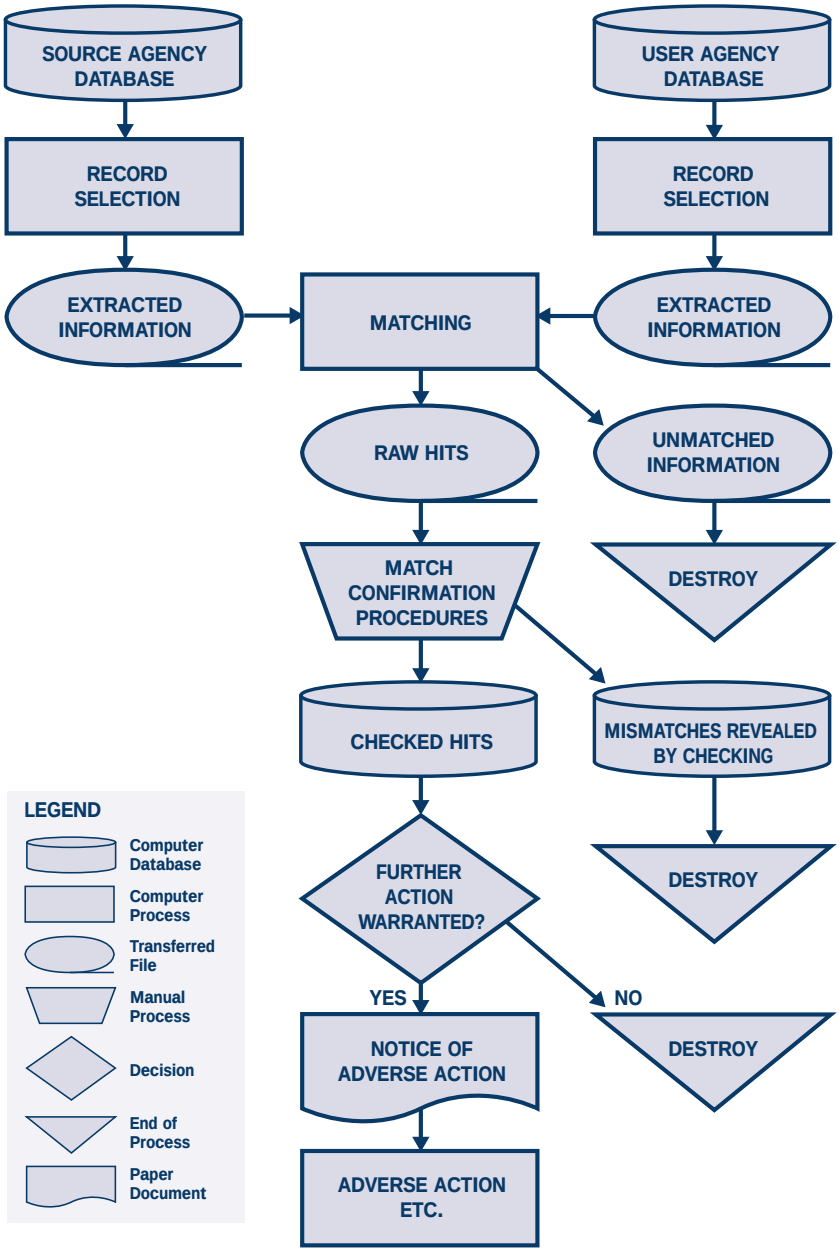
The process begins with two databases, one at the source agency and the other with the user agency (in more complicated programmes there may be multiple databases involved). From each database certain records are selected. For example, a department may wish to select only those of its records relating to people who have been involved in a recent transaction or activity (such as claiming a particular benefit or departing the country). Certain information is extracted from the records that have been selected (sometimes called "data scrubbing"). For example, the agency may have 20 items of data relating to individuals who have claimed a benefit or left the country but only five of these may be needed to be extracted for the programme.[1]

The extracted information is sent for matching. This is an automated process of comparison of the lists of data received from each agency. The process may be undertaken by the source or user agency or by a separate matching agency. Whichever agency undertakes the process, the information being matched is kept physically separate from operational records until checking processes are complete.[2] It is important that unverified information not be added to an individual's file until it is confirmed that the information does indeed relate to that individual and that it is accurate and relevant.

An algorithm is developed and used to establish what constitutes a successful match or "hit".[3] An algorithm is a process or set

1 Typically the statutory information matching provision and the Technical Standards Report (required by information matching rule 4) both limit the information which may be utilised in an authorised programme.
2 The use of on-line computer connections in matching programmes is prohibited: matching must be carried out "off line" and not be used to update live data on an agency's database - information matching rule 3.

Figure 2: Information Matching Process



of rules used for problem solving. For example, the algorithm may establish as a match – being records from the two sources likely to relate to the same person – cases where the full name, date of birth and address are all the same. However, most algorithms allow for the identification of "likely" matches even when all data do not exactly correspond. An algorithm might, say, allow for partial matches where the surname and date of birth are the same even where the first name differs. An algorithm may allow for differences in the spelling of names or use a number of letters from the stem of a word without requiring the whole word (such as the name) to match. The process is one of inference: the match is judged *likely* to relate to the same person, but that cannot be said to be *certain* without further confirmation.

Depending on the nature of the programme, the user agency may be interested in entries which appear on both lists of extracted information or the interest may be in entries which appear on one list but not the other. The process of comparison is essentially the same in both cases. The matching results in a list of raw hits to be followed up. The information which does not show a "hit" of interest should not need to be retained.[4]

The raw hits are put through appropriate confirmation procedures.[5] There are a variety of checks that might be made at this point in the process. A typical one might be to manually check original records held by the user agency. The confirmation procedures may reveal some mismatches which are then destroyed.[6]

The resultant checked hits may be used as a basis for taking action against individuals. The hits should be acted upon, if at all, in a reasonable time. The information must not be allowed to become out of date since this may prejudice the individuals concerned.[7] Unverified information derived from matching must not be allowed to enter and remain upon administrative files.[8]

---

3 Information matching rule 4 requires the matching algorithm to be documented in a Technical Standards Report. Other aspects of the match are also documented there or in the information matching agreement required under Privacy Act, s.99.

4 Where the matching does not reveal a discrepancy, information matching rule 6 requires the relevant information to be destroyed.

5 The agencies involved in a programme are required to establish reasonable procedures for confirming the validity of discrepancies before any agency seeks to rely on them as a basis for action in respect of an individual - information matching rule 5.

6 Information disclosed pursuant to a match which reveals a discrepancy but is no longer needed for taking adverse action against an individual must be destroyed as soon as practicable - information matching rule 6(2).

7 The information matching controls require that a decision as to whether to take action must be taken within 60 days or the information must be destroyed - Privacy Act, s.101.

8 Nor may separate permanent databases of programme information be created - information matching rule 7.

It is not advisable to act solely on the basis of an apparent discrepancy produced by a match even with some in-house checking completed. In fairness the material should be notified to the individual concerned before action is taken against that person. This allows an opportunity for the data to be challenged so as to prevent an injustice. People should not be "presumed guilty" on the basis of unverified inferences drawn from the matching process. Notice is an especially important safeguard where the matching process might have wrongly associated records relating to different individuals.[9]

This is simply a basic outline of the operational safeguards. There are a number of others. From this year, the Privacy Commissioner has established a full time position of Data Matching Compliance Officer. While that officer is also involved in the authorisation and evaluation processes, the core of the role is in relation to ensuring compliance with the Privacy Act's operational requirements for authorised information matching programmes.

International data matching: mutual assistance in social security

The Social Welfare (Transitional Provisions) Amendment Bill, introduced into Parliament during the year, would establish a framework for authorising new information matching programmes between the department administering the Social Security Act (DWI) and its overseas counterparts. There will be further associated information matching between DWI and the Inland Revenue Department to give effect to the arrangements with overseas social security authorities and to utilise information for tax purposes. The objective of these measures is to:

- allow social security agreements entered into by New Zealand with other countries to include mutual assistance provisions for the recovery of the social security debts of either country;

- allow such agreements to include mutual assistance provisions for the exchange of information for social security purposes.

9 If it is intended to take adverse action based upon a discrepancy revealed by a programme, the user agency must first serve written notice on the individual under s.103 of the Privacy Act giving details of the discrepancy and the proposed adverse action and allowing the individual 5 working days to show reason why such action should not be taken - Privacy Act, s.103.

The initiative for such an arrangement had followed an approach from the Netherlands. Without such provision the Netherlands would cancel its social security arrangements with New Zealand.

I examined the proposal, as outlined in an Information Matching Privacy Impact Assessment (IMPIA) by the Ministry of Social Policy. I submitted a report to the Minister of Justice on the draft implementing legislation in April 2000 just before the bill was to be introduced into Parliament. The legislation had a number of features which were unprecedented in other New Zealand information matching legislation. Unique aspects included:

- the involvement of overseas government agencies as the source of information provided for matching;
- the disclosure to overseas government agencies of information about New Zealand residents for matching;
- according DWI a "middle man" role to obtain tax information for overseas agencies from IRD.

The programmes to be established under the new law were not themselves to have Part X applied to them in all respects because one party to the data matching equation, the overseas government agency, would not be subject to the New Zealand Privacy Act. However, the bill sought to provide individuals with appropriate protection of their privacy through protections equivalent to the information matching controls in Part X of the Privacy Act.

Having undertaken my examination of the proposal, I was generally satisfied with the approach taken. I had some concrete information on which to judge the framework in the form of a proposed agreement with the Kingdom of the Netherlands. However, that arrangement is likely to be less troubling than certain others that might arise in the future: the Netherlands has a data protection law which would apply to any information received and would accord similar protections and rights as the New Zealand Privacy Act. I would be unlikely to look with such favour from a privacy perspective on a programme which would disclose information to a jurisdiction without equivalent privacy or data protection law.

Amendments were made to the bill before it was introduced into Parliament to meet the issues I raised in my report. I have continued discussions with the Ministry of Social Policy about the

implementation arrangements for the proposed first programme with the Netherlands but the bill remained before Parliament at the end of the year.

PROGRAMME BY PROGRAMME REPORTS

Introduction

Section 105 of the Act requires me to report annually on each authorised programme carried out during the year. This year's report covers 17 authorised programmes of which 12 operated during the year.

I have entitled each programme with the names of the specified agencies involved followed by a description. The agency whose only role is as a source of information is named first. The agency making use of the discrepancies produced by the match is named second. For instance, in the "IRD/Accident Insurance Regulator Employer Compliance Match" IRD is given first as the source agency. The Regulator as user agency is given second. This programme is described as an "employer compliance match" which indicates something of its nature and distinguishes it from the "sanction assessment match" involving the same agencies.

I have classified each programme by one or more of eight primary purposes. The currently authorised programmes can be characterised as follows:

- ***confirmation of eligibility or continuing eligibility*** for a benefit programme, or compliance with a requirement of a programme -10 programmes;

- ***detection of illegal behaviour*** by taxpayers, benefit recipients, government employees etc (e.g. fraudulent or multiple claims, unreported income or assets, impersonation, omissions, unauthorised use, improper conduct, conflict of interest) - 6 programmes;

- ***updating of data*** in one set of records based on data in another set - 3 programmes;

- ***location of persons*** with a debt to a government agency - 3 programmes;

- ***detection of errors*** in programme administration (e.g. erroneous assessment of benefit amounts, multiple invoicing) - 1 programme;

- ***identification of persons eligible for a benefit*** but not currently claiming that benefit - 1 programme;

- ***data quality audit*** - 0 programmes;

- ***monitoring*** of grants and contract award processes - 0 programmes.[10]

Each entry in the balance of the report commences with basic summary information about the programme being reported upon. A description of the object of the programme and the manner in which it is carried out follows. There is discussion of the operation of the match during the year and, in most cases, a table of results and some brief commentary on those results. As required by the Privacy Act, I express my opinion as to the extent of each programme's compliance during the year with sections 99-103 and with the information matching rules.

In this part of the report, I use various abbreviations and acronyms. The main ones are:

ACC	Accident Compensation Corporation
Courts	Department for Courts
Corrections	Department of Corrections
CSC	Community Services Card
Customs	NZ Customs Service
DWI	Department of Work and Income
EEC	Electoral Enrolment Centre
IMPIA	Information Matching Privacy Impact Assessment
IRD	Inland Revenue Department
NDMC	National Data Match Centre of DWI
NZIS	New Zealand Immigration Service
Regulator	Accident Insurance Regulator
VOS	Verification of Study

10 The eight categories were suggested by Dr Roger Clarke of the Australian National University. I have included the two categories for which there are no local examples merely to show the other uses to which matching has been put elsewhere.

The reports are set out in the following order:

Matches with DWI as user agency

A. Corrections/DWI Inmates Match
B. Customs/DWI Arrivals & Departures Match
C. IRD/DWI Commencement/Cessation Match
D. IRD/DWI Debtor Address Match
E. Employers/DWI Section 11A Social Security Act Match
F. IRD/DWI Community Services Card Match
G. Educational Institutions/DWI Loans & Allowances Match

Matches with other departments as user agency

H. DWI/Courts Fines Defaulters Address Match
I. DWI/IRD Family Support Match
J. NZIS/EEC Unqualified Electors Match
K. IRD/Accident Insurance Regulator Employer Compliance Match
L. IRD/Accident Insurance Regulator Sanction Assessment Match

Matches which did not operate during year

M. IRD/Courts Fines Defaulters Address Match
N. Corrections/ACC Inmates Match
O. ACC/IRD Child Tax Credit Match
P. IRD/ACC Earners Match
Q. Labour/DWI Immigration Match

General comments about the main DWI programmes

Before turning to the specific programmes I offer some brief global comments on three of the most important matches.

In previous annual reports, I have totalled certain figures and collated comments which apply to the conjoined major information matching programmes run by the National Data Match Centre (NDMC). There were four such programmes: the Customs match of arrivals and departures, the Inland Revenue match with employment commencement/cessation, the Corrections match with prison admissions, and the Education match with student allowance recipients. A major reason for combining these four was that the NDMC centre was unable to separate out the costs for running the individual programmes, so the only way to compare the costs with the moneys recovered through the operation of the programmes was to lump them together.

This year there are only three such programmes, not four. The "missing" programme is the one with the Ministry of Education which, since the administration of student allowances has been moved to DWI, is no longer necessary as the co-ordination between student allowances and other social welfare benefits which may be claimed by the recipients is now handled directly when the individual applies for an allowance or other benefit. For this reason, although the Education match was never a large part of the NDMC's work, it is not meaningful to compare this year's figures with those of prior years.

Most elements of the costs of operating the NDMC programmes are still reported to me as global figures, rather than being broken down between the different programmes. This year the allocation as between the headings "general expenses" and "overheads" has also been changed, so again the comparison with earlier years' figures is not useful. I therefore cite the total figures only:

TABLE 11: COMBINED TOTAL FIGURES FOR THE THREE MAIN DWI NDMC PROGRAMMES	
Overpayments established	$28,782,047
Penalties applied	$7,107
Cost of matching operation	$6,531,957
Debt recovery costs (see note below)	$1,328,880
Debts recovered	$9,856,131

Note that debt recovery cost is an estimate provided by DWI which applies only to the non-current debt recovery activity, i.e. obtaining payment of debts owed by individuals who are not currently receiving any social welfare benefit. The non-current debt recovery accounts for almost 70% of the total money recovered during the year, and I assume that the cost of recovering debts by deduction from current benefit payments is a much cheaper process than pursuing the non-current debtors.

The penalties imposed on cases discovered through the three information matching programmes are almost negligible: 16 penalties out of 30,992 overpayments. Given that DWI continues to demonise such overpayment cases with the words "crime" and "fraud", it seems extraordinary that the overwhelming majority of cases attract no sanction whatsoever.

Continuing to build upon the significant improvements in reporting to me - which I acknowledged last year - the NDMC has again produced more thorough and reliable reports than I have previously enjoyed. One feature this year is the recording and reporting of challenges to match results; now that I can start to see the real incidence of these challenges, a clearer picture is emerging of the potential for inaccuracy in these individual programmes and of the value of the s.103 notice procedure. Using some projections from the figures reported, it appears that the incidence of successful challenges to the total overpayments produced by the programme concerned is approximately as follows:

Customs match:	1 case in 180;
Inland Revenue match:	1 case in 40;
Corrections match:	1 case in 850.

I will encourage DWI to continue to monitor and record such challenge figures with an eye to establishing patterns which might enhance accuracy of the matching processes.

Matches with DWI as user agency

A. Corrections/DWI Inmates Match

CORRECTIONS/DWI INMATES MATCH	
Information matching provision	Penal Institutions Act 1954, s.36F
Year authorised	1991
Commencement date	April 1995
Match type	Confirmation of continuing eligibility
Unique identifiers	None
On-line transfers	None

The Corrections/DWI Inmates Match[11] 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 the Department of Work and Income.

The information is compared by name and date of birth. Matched individuals are sent a notice advising them that, unless they produce proof to the contrary, the benefits which they are receiving from DWI will cease and any overpayment found to have been made will be established as a debt to be repaid to DWI.

Results

TABLE 12: CORRECTIONS/WINZ INMATES MATCH – 1998-2000 RESULTS		
	1998/99	**1999/00**
Number of runs	50	53
Number of records compared	23,731	13,640
Number of "positive" matches	9,279	5,771
Legitimate records (no adverse action taken)	5,420	3,118
Notices of adverse action issued	3,886	2,658
Debts established (number)	4,015	2,545
Overpayments established	$2,749,023	$1,129,452
Challenges	3	4
Challenges successful	0	3

The most obvious development in the statistical results for this programme is a major reduction in the number of records compared. These records originate in the Department of Corrections, which this year implemented a new database system ("OIMS" - Offender Integrated Management System). Unlike its predecessor system, this database distinguishes between a prison admission resulting from transfer from another prison, and a whole new admission to the prison system. Thus DWI is spared the significant number of records it used to receive where a prisoner had merely transferred, and almost certainly had had any benefit payments stopped some time before. This change is believed to account for the significant (42%) reduction this year in the records compared by this information matching programme.

If that was the only change in the system or the underlying facts, I would expect to see a corresponding rise in the proportion of records which lead to the establishment of an overpayment debt, as the number of new entrant prisoners who are in receipt of a benefit would presumably stay the same. Instead, however, the rate of positive matches among the records compared has gone down slightly, with the result that the number and value of debts established by this programme has fallen markedly. Most of those overpayments which are thus established arise from the unemployment benefit. I would not like to speculate on the reason for this decline.

Despite that decline in the number and value of benefit overpayments detected among those entering prisons, I am satisfied that this information programme is still worthwhile in monetary terms as well as helping to protect the integrity of the benefit system.

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

11 To assist in comparison with material in earlier annual reports where there has been change, the previous names used for particular programmes are given in footnotes. In particular, the Department of Work and Income has recently ceased to refer to itself as Work and Income NZ or WINZ. This match has formerly been referred to as the "Corrections/WINZ Penal Institutions Match", the "Corrections/NZISS Match" or simply "*the* Corrections Match".

B. Customs/DWI Arrivals & Departures Match

CUSTOMS/DWI ARRIVALS & DEPARTURES MATCH	
Information matching provision	Customs and Excise Act 1996, s.280
Year authorised	1991
Commencement date	June 1992
Match type	Confirmation of continuing eligibility
Unique identifiers	None
On-line tranfers	None

The Customs/DWI Arrivals & Departures Match[12] 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 can vary from benefit to benefit.

The programme operates by a transfer of passenger arrival and departure information once a week from NZ Customs Service to DWI. The information is compared with DWI's database of beneficiaries by name, date of birth, and gender. The information provided to DWI also includes passport number, flight number, country of citizenship, and dates of arrival or departure.

DWI then checks its records to determine whether there has been an explanation given 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 DWI 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, DWI does not issue a notice of adverse action until the requisite period passes and the individual remains out of New Zealand.

12 Formerly referred to as the "Customs/WINZ Arrivals/Departures Match", "Customs/NZISS Match", "Customs/DSW Match" or simply "*the* Customs Match".

Results

TABLE 13: CUSTOMS/DWI ARRIVALS & DEPARTURES MATCH – 1997-2000 RESULTS [13]			
	1997/98	**1998/99**	**1999/00**
Number of runs	52	52	52
Number of records received from Customs	3,919,190	5,646,430	6,086,485
Number of "positive" matches	23,888	24,912	26,989
Legitimate records (no adverse action taken)	5,474	7,187	7,183
Notices of adverse action issued	13,539	18,165	19,797
Debts established (number)	10,429	13,577	12,203
Overpayments established	$5,240,816	$7,222,958	$5,972,158
Challenges	9	33	84
Challenges successful	*	28	64
* Figure not available			

The number of arrival and departure records supplied by Customs continues to grow, representing more travel movement as well as more comprehensive capture of records.

This well-established information matching programme works quite smoothly as far as I am aware. Liaison between DWI and Customs has been formalised with a new Memorandum of Understanding, and this is causing more attention to be given to communication issues. A revised information matching agreement and Technical Standards Report is to be produced to update the existing documentation, which has been subject to successive variations over time. I welcome this sort of initiative.

The pattern of the overpayments established by this match has not changed much over recent years, but is of interest. The overpayment total and the median individual overpayment for each type of social welfare benefit are shown below.

13 The 1997/98 figures are as at 30 June 1998, the 1998/99 figures as at 31 August 1999 and the 1999/2000 figures as at 17 August 2000.

TABLE 14: CUSTOMS/DWI ARRIVALS & DEPARTURES MATCH – 1999/2000 – BREAKDOWN BY BENEFIT TYPE			
Benefit type	**Number**	**Total overpayments $**	**Median overpayment $**
Unemployment	9,786	3,624,111	332
Sickness	1,072	411,977	323
Training	89	23,698	215
DPB	957	1,401,264	1,559
Invalid	109	108,725	905
Widows	87	73,942	641
Orphans	28	17,468	548
Superannuation	75	310,969	4,872
Total	12,203	$5,972,158	n/a

The high median overpayment value for NZ superannuation is due to the rule that superannuation recipients are allowed to be overseas for up to six months without affecting their pension entitlement but, if they stay overseas beyond that limit, the superannuation for the entire overseas period usually becomes repayable.

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

C. IRD/DWI Commencement/Cessation Match

IRD/DWI 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 behavior
Unique identifiers	Tax file number
Online transfers	None

The IRD/DWI Commencement/Cessation Match[14] is designed to detect those who are receiving a benefit and working at the same time. The programme operates by an exchange of information approximately six times a year between the Inland Revenue Department and the Department of Work and Income. DWI 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 DWI. Any matched individuals are then investigated further by DWI to determine whether the individual has earned amounts over the limit set for the relevant benefit. A check of the records held by DWI is done to determine whether there is already an explanation for the match on DWI'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 DWI 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 in one of three ways:

- all those individuals who commence or cease receiving a benefit in the period since the last match;

14 Formerly referred to as the "IRD/WINZ Commencement Cessation Match", the "IRD/NZISS Commencement/Cessation Match", the "Commencement/Cessation Match" or simply "the IRD Match".

- any Area Benefit Crime unit may nominate specific individuals whom they are investigating;

- one sixth of all those enrolled with DWI.

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 DWI will have had their records matched with IRD at least once.

Results

TABLE 15: IRD/DWI COMMENCEMENT/CESSATION MATCH – 1998-2000 RESULTS

	1998/99	1999/00
Number of runs	6	7
Number of records compared	432,772	490,151
Number of "positive" matches	113,370	226,659
Legitimate records (no adverse action taken)	90,840	164,272
Notices of adverse action issued	36,622	38,774
Debts established (number)	14,486	16,244
Overpayments established	$24,300,764	$21,680,438
Challenges	263	765
Challenges successful	98	211

This information matching programme is easily the most valuable of the anti-fraud matches carried out in New Zealand, measured in terms of the overpayment amount discovered. It has been going for over 7 years now in more or less the same form, and appears to have reached a relatively high level of efficiency and control.

Minor system improvements are made from time to time, and an example of these which has occurred this year is the automation of letters which are to be sent to employers where discrepancies which meet the Department's criteria are discovered. The letter seeks confirmation and further details from the employer where a benefit recipient appears to have been working at the same time as claiming and receiving a benefit inconsistent with that employment. DWI's computer system incorporates an easy method by which staff can suppress the sending of that letter if the individual concerned responds to the s.103 notice (which warns them of the

intention to approach the employer) and opts to produce the necessary details of earnings directly to DWI.

With the long experience of this matching programme and with its operation highly controlled by the centralised National Data Match Centre, it might be thought that few surprises could now be encountered in the way that it runs. However, the figures for this year show the effect of just such a surprise. There are much higher figures this year for "positive" matches and for "legitimate records". What this means is that, compared with previous years, a substantial additional number of "raw hits" indicated that an individual was in employment whilst receiving a benefit, but upon some investigation this was found to be "legitimate". The anomalous figures are in part the result of an amusing, but noteworthy, system problem.

Due to changes in the way Inland Revenue conducts its business and keeps its records, taxpayers receiving payments of taxable income from insurance companies (including ACC) and from the DWI itself suddenly began showing up in this match as if they were employees of the payer. In the case of insurance payments, this information is potentially very useful to DWI, as some such insurance income may be inconsistent with continued receipt of a social welfare benefit. The receipt of benefits from DWI, however, is not something that DWI wishes to learn from IRD records. The problem first occurred in late August 1999, was spotted and contained so that no form of adverse action was taken against any of the individuals thus identified, and a system amendment was effected in December 1999 to stop such payments showing as discrepancies.

DWI and ACC are now working together to formalise liaison in dealing with those cases where an ACC payment compromises entitlement to a social welfare benefit, as revealed through the revised IRD system.

A further batch of additional "positive" matches and legitimate records is believed to arise from another change in Inland Revenue's procedures, which has unwittingly produced many errors in the employers' monthly reports to IRD, flowing through to create multiple records for the same individual employee as reported to DWI in this information matching programme. I am advised that Inland Revenue is aware of the problem and will presumably work to correct it. In the meantime, the NDMC staff of DWI only progress the record that shows the earliest employment start date and are

coding as “legitimate” the remaining records from that same employer for that same employee.

The point to be taken from this event is that, whenever any agency interconnects to another through an information matching programme, all parties to the programme must be on guard to check that any changes to their internal information systems do not produce changes in output to the other agency unless the change has been well explored and agreed in advance.

A complaint investigated during the year highlighted that notices sent by the Department in relation to this programme did not meet all the requirements of s.103. Notices are required to be given to individuals before any adverse action is taken against them. Section 103 is therefore one of the key safeguards in the information matching controls and any non-compliance in the more than 38,000 notices issued during the year is obviously a serious matter. The complaint in question raised wider issues than merely the content of the s.103 notice and it was still being dealt with at the end of the year. However, I conveyed to the Department my opinion that the notice was defective in several respects. In the coming year, one of the tasks of my new Data Matching Compliance Officer will be to work with the NDMC to ensure that this notice, and any other similarly defective notices, become fully compliant.

On the basis of the information which has been supplied to me, I am satisfied that this programme has been conducted in accordance with ss.99 – 102 of the Privacy Act and the information matching rules. I have already noted the partial non-compliance with s.103.

D. IRD/DWI DEBTOR ADDRESS MATCH

IRD/DWI DEBTOR ADDRESS MATCH	
Information matching provision	Tax Administration Act 1994, s.85
Year authorised	1993
Commencement date	November 1994
Match type	Location of persons
Unique identifiers	Tax file number
On-line transfers	None

The IRD/DWI Debtor Address Match[15] is designed to provide DWI with up-to-date addresses from IRD for those who owe money to DWI. 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 DWI has lost contact. The programme is one part of DWI's process of collecting debts established by the other DWI information matching programmes, as well as from other DWI operations.

Results

TABLE 16: IRD/DWI DEBTOR ADDRESS MATCH – 1997-2000 RESULTS			
	1997/98	1998/99	1999/00
Number of runs	5	6	5
Debtors sent for matching (A)	256,324	342,697	293,057
Average number of debtors per run	51,625	57,116	58,611
Matched by IRD (B)	230,174	304,552	261,672
% of debtors sent (B/A)	89.8%	88.9%	89.2%
Matches found useable (C)	45,047	94,115	57,485
% of debtors sent (C/A)	17.6%	27.5%	19.6%
% of those matched by IRD (C/B)	19.6%	30.9%	22.0%
Letters sent out (D)	7,708	8,534	3,444
% of those matched by IRD (D/B)	3.3%	2.8%	1.3%
% of matches found useable (D/C)	17.1%	9.1%	6.0%
Letters not returned (presumed delivered) (E)	6,482	7,612	3,199
% of letters matches found useable (E/C)	14.4%	8.1%	5.6%
% of letters sent out (E/D)	84.1%	89.2%	92.9%

15 Formerly referred to as the "IRD/WINZ Debtor Address Match", the "IRD/NZISS Address Match", the "IRD/DSW Address Match" or simply "the Address Match".

The proportion of "matches found useable" which resulted in letters being sent out has dropped noticeably this year from the earlier performance achieved by this matching programme. Letters are not sent out if, after further scrutiny of the matches which the programme has produced, the address supplied by IRD is apparently invalid or out of date.

If this drop-off in the rate of useful results continues, there will come a time shortly when the programme should be reconsidered because it will not pay for itself. That is not to say that the programme should definitely be discontinued just because the monies collected with its assistance are not sufficient to pay for its operation, but it must cast the continued utility and value of the programme into question.

Although the process has hardly been going on long enough to have affected this year's figures, there is reason to expect that IRD's address data will now get further out of date every year, because the new income tax system has largely done away with the need for individuals to submit tax returns and thereby update Inland Revenue's address details. This new factor can be expected to accentuate a downwards trend in the benefits obtained from this information matching programme.

As with any information matching programme which aims to assist collection of old debts through tracing the debtor, the monetary result will only come some months after the initial matching operation. The individual debtor must be contacted and persuaded either to pay or at least to enter into (and continue to comply with) an arrangement for payment by instalments. Because of this delay in receipt of tangible benefits, the direct comparison of costs and benefits is either done much in arrears or is based upon estimation taking into account any evident trends. I expect to see a reappraisal of the future of this programme carried out within the next year or two.

In the meantime, on the basis of the information reported to me, I am of the opinion that the programme has been operated in accordance with sections 99 to 103 of the Act and the information matching rules.

E. Employers/DWI Section 11A Social Security Act Match

EMPLOYERS/DWI SECTION 11A SOCIAL SECURITY ACT MATCH	
Year authorised	1993
Match type	Detection of illegal behaviour
Unique identifiers	Tax file number
On-line transfers	None

Section 11A of the Social Security Act 1964 authorises DWI to request information from employers about their employees or a specified class of employees (including former employees).[16] The information may include names and addresses and tax file numbers. Section 11A(3) prevents DWI requesting information from the same employer within a 12 month period. The information thus obtained may then be compared with records of social security benefits paid out. Any discrepancies found are dealt with in terms of section 11A. Sections 11A(6) and (7) effectively bring the operation of the information matching programme under Part X of the Privacy Act for most purposes.

Results

TABLE 17: EMPLOYERS/DWI SECTION 11A SOCIAL SECURITY ACT MATCH – 1997-2000 RESULTS			
	1997/98	**1998/99**	**1999/00***
Matches approved	109	75	89
Matches completed	109	69	56
Matches not completed	0	6	33
Details of completed matches			
Total employees checked	29,373	15,266	13,500
Cases investigated	3,810	2,278	774
Benefits cancelled or adjusted	2,165	1,377	543
Total cost	$235,291	$106,574	$19,762
Total savings	$3,282,604	$1,682,282	$1,024,048
Net savings	$3,047,313	$1,575,709	$1,004,286
***As at 19 July 2000**			

16 This match has previously been referred to as the "Section 11A Social Security Act Match".

Table 17 shows the results of the programme for the last three years. However, it is difficult to compare each year's results as each year is at a different stage of completion. All of the matches approved in 1997/98 have been completed as have most, but not all, of the following year's. About a third of the matches approved in 1999/2000 remain current and have not been completed as at late July 2000. Accordingly, the following table sets out results for the last two years in a broadly comparable position in the cycle.

TABLE 18: EMPLOYERS/DWI SECTION 11A SOCIAL SECURITY ACT MATCH – 1998-2000 COMPARABLE INTERIM RESULTS

	1998/99 (as at 6/8/99)	1999/00 (as at 19/7/00)
Matches approved	79	89
Matched completed	41	56
Matches not completed	38	33
Total cost	$18,458	$19,762
Total savings	$658,586	$1,024,048
Net savings	$640,128	$1,004,286
Net savings per completed match	$15,613	$17,934

Bearing in mind the numbers of completed matches, the results are fairly consistent for the two years.

During the year some work was undertaken towards reviewing the operation of this match pursuant to s.106 of the Privacy Act. It was not possible to complete that review during the year but the opportunity was taken to circulate a questionnaire to a number of employers who had received s.11A demands for information for matching purposes. Analysis of the responses to that questionnaire will be completed next year as part of the s.106 review.

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

F. IRD/DWI Community Services Card Match

IRD/DWI COMMUNITY SERVICES CARD MATCH	
Information matching provision	Tax Administration Act 1994, s.83
Year authorised	1991
Commencement date	1992
Match type	Identification of persons eligible for a benefit not currently claiming
Unique identifiers	Tax file number
On-line transfers	None

The IRD/DWI Community Services Card Match[17] is an information matching programme in which the IRD supplies DWI with tax credit information, for the purpose of allowing DWI to identify those individuals whose income is at a level which makes them eligible for a Community Services Card (CSC). A CSC entitles the holder to subsidised health care. Over 300,000 cards are issued each year with a total of about 1.3 million on issue at any one time.

The information provided by IRD is matched against the income limits for the card. The income limits vary depending upon the number of dependent children. Each exchange generates:

- a letter to a person matched advising that he or she is over the income threshold for a card; or
- a letter advising that the person is within the threshold for the card and enclosing an application form for a card which may be completed and returned; or
- if a current CSC is already held, a renewal flag is placed upon SWIFTT, DWI's computer system for records on current beneficiaries, so that when the existing card expires a new card is automatically generated for eligible cardholders.

The information matching programme allowed costs to be saved by automating assessment and issue of some CSCs. Information matches usually occur fortnightly. The number of cases in each run varies, with on average about 10,000 cases each time.

17 Formerly referred to as the "IRD/WINZ Community Services Card Match", the "IRD/NZISS Community Services Card Match", or the "Community Services Card Match".

I have not required any formal reports from DWI or IRD this year. I have no reason to believe that the programme does not comply with ss.99-103 of the Privacy Act and the information matching rules.

G. Educational Institutions/DWI Loans & Allowances Match

EDUCATIONAL INSTITUTIONS/DWI LOANS & ALLOWANCES MATCH	
Information matching provisions	Education Act 1989 • s.226A – Institutions • s.238B – Private training establishments
Year authorised	1998
Commencement date	• 1998 – Allowances • 1999 – Loans
Match type	• Confirmation of eligibility and continuing eligibility • Updating of data
Unique identifiers	• DWI customer number • Student identification numbers
On-line transfers	None

This programme operates between the Department of Work and Income and educational service providers.[18] The purpose of the programme is to enable DWI to obtain the enrolment information required to assess a student's entitlement to receive a student allowance, student loan or both, which are payable in terms of the criteria prescribed under regulations. The data provided by educational institutions enables DWI to:

- verify that a student is undertaking a programme of study which has been approved by the Ministry of Education for student allowance and loans purposes;
- determine whether the student is full time;
- confirm start and end dates of the student's programme; and
- confirm any vacation periods exceeding three weeks during the student's period of study.

Upon receipt of data from an institution DWI decides whether to grant an allowance or loan, or decline an allowance or loan on the grounds that:

18 The programme was referred to in last years annual report as the "Tertiary Institutions/WINZ Student Allowance Match."

- the student is not enrolled in an approved programme of study; or

- the student is not studying full-time.

This part of the matching programme is known by the participants as Verification of Study (VOS).

Results

This programme is an example of the use of information matching for verifying the eligibility of an individual for a certain benefit. The Department of Work and Income took over the administration of student allowances and implemented this matching programme in late 1998. In late 1999 DWI took over the administration of student loans, and extended the existing information matching programme to accommodate the loans function in parallel with the allowance function. The number of student loan recipients is much greater than the number of student allowance recipients, but there is a large overlap. There were approximately 62,000 applications for loans but not allowances, approximately 17,000 applications for allowances but not loans, and approximately 59,000 applications for both loans and allowances. Thus the extension of this information matching programme from allowances to both loans and allowances was a major change in the size of the operation.

With both student allowances and student loans, one of the criteria for granting them is enrolment in an approved tertiary education course. There are innumerable qualifying courses, offered by over 700 separate tertiary education institutions which range from the universities through to small private training establishments. Rather than requiring the student applying for a loan or allowance to produce proof of enrolment, DWI uses an information matching process to contact the tertiary education provider directly for the necessary verification of study enrolment.

On a weekly cycle, DWI sends to an education institution the details of those applicants who have claimed to be enrolled with that institution for a course which qualifies for the allowance or loan in question. The institutions match the details of those applicants with their enrolment records and report back to the Department accordingly. Thus the matching process is actually carried out by the tertiary education providers, with results fed back to the DWI for actioning.

Each tertiary education provider has entered into a standard form of information matching agreement with DWI. The larger institutions, as may be expected, carry out the information matching process in an automated routine, whereas the smaller ones presumably make just a manual check of their enrolment records and produce a manual form of feedback. Of the 720 or so education providers who operated this information matching programme this year, only around 20 have fully computerised systems for doing so, but those 20 accounted for some 78% of all the verifications.

There were numerous and well-publicised problems with the processing of student loan applications in late 1999 and early 2000. The verification of study, accomplished by the information matching programme, forms a small but vital part of the process. A report on the various problems was prepared for the Ministry of Social Policy in June 2000 (the Erenstrom Report). I was not consulted by the authors of that report, but I have obtained a copy and was interested to see that several education providers evidently made comments that were less than complimentary as to the management of the introduction of the VOS information matching process but there are no comments cited against the process itself. If I understand the report correctly, there is a theme that the process of change would have benefited from more advance testing by means such as pilot schemes, more consultation and liaison with those concerned, and more readiness of resources and attitudes to cope with practical problems in the introduction of a new system. These are all sound points which I make repeatedly to any agencies introducing information matching programmes.

Apart from the start-up difficulties in introducing the existing student allowances programme to the greater task of dealing with student loans, the actual information matching process appears to have worked satisfactorily once it got well under way. However, this match has a very pronounced and unavoidable annual workload peak at the beginning of each academic year, so the test of whether or not there are still some practical problems in the system will not come until the first quarter of 2001.

In order to show the effect of the inclusion of student loan application verifications as well as the annual workload peak, I have set out the key indicators of the programme for each quarter of the 1999/2000 year in Table 19.

TABLE 19: EDUCATIONAL INSTITUTIONS/DWI LOANS & ALLOWANCES MATCH – VOS RESULTS 1999-2000				
	7-9/99	10-12/99	1-3/00	4-6/00
Total VOS requests made	19,066	16,708	343,665	101,545
Individual applicants involved	10,935	9,255	112,836	37,332
Positive matches achieved	16,708	15,350	289,098	42,057
Confirmed eligibility	11,405	5,218	147,791	60,127
Number of providers involved	582	380 appr	719	720
VOS successful first time (see below)	69%	56%	43%	59%
More than 5 VOS attempts	4%	2%	0%	13%

If the educational institution does not respond with matching details within a week, a further VOS is sent out by DWI. Sometimes the failure to match and advise the Department of Work and Income is because the student has not enrolled (as yet), sometimes it is because the student name does not match, and sometimes because the course enrolled for is not shown as having been approved for loan or allowance eligibility. After a number of VOS attempts have proved unsuccessful, the student applicant is notified pursuant to s.103 of the Privacy Act that the application is going to be turned down, and is given an opportunity to show why that should not happen. More than five attempts to verify a particular application suggests to me that something was wrong with the initial information either in DWI or in the education provider, and the high figure for these multiple attempts in the June 2000 quarter is something I am taking up with the Department.

The other key purpose of the match is to provide DWI with the study results of students who have received payment of an allowance. Students must pass more than half of the programme for which they received an allowance, otherwise their future entitlement to any allowances is suspended. This part of the programme is known by the participants as Results of Study (ROS). Although the framework for ROS has been put in place, I was not given any information to indicate that this part of the programme operated during the year. I understand it is planned to be implemented in 2000.

Notification about this information matching programme is given to student applicants when they apply. I have not received any complaints about this programme so far. On the information

provided to me I am satisfied that the programme, despite initial difficulties in implementation, has been operated in accordance with sections 99 to 103 of the Privacy Act and with the information matching rules.

Matches with other departments as user agency

H. DWI/Courts Fines Defaulters Address Match

DWI/COURTS FINES DEFAULTERS ADDRESS MATCH	
Information matching provision	Socal Security Act 1964, s.126A
Year authorised	1996
Commencement date	1998
Match type	Location of persons
Unique identifiers	None
On-line transfers	None

The DWI/Courts Fines Defaulters Address Match[19] is an information matching programme in which the Department for Courts is to be supplied with address information by the Department of Work and Income 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.

Results

There were five runs of this programme in the 1999/2000 year, compared with just two in the previous year. Meaningful reports on the programme can only be generated some months after a particular matching run, because the process of following up on an apparent "hit" (that is, a new address for an old debtor) inevitably takes considerable time to reach the point where payment is recovered or a "time to pay agreement" is entered into. If the results for all matching runs made during the year are reported as at (say) September, appreciable year-to-year variations might reflect nothing more than the rate of progress in processing results of the later matches covered. For that reason, the statistical results of a match run are not reported to me until six months have elapsed, by which time much of the follow-up action can be expected to have been taken and a meaningful proportion of outcomes collated, and again at 12 months when all reportable action should have been completed. 1999/2000 is the first year in which this system of six-monthly reports has been used, so it is not possible to compare the statistics directly with those of the prior year.

19 Formerly referred to as the "WINZ/Courts Address Match" and the "NZISS/Courts Address Match".

Last year I reported that processing or system faults dogged one of the two match runs of this programme in 1998/99. This year, again, there have been some problems and one of the runs had to be abandoned and re-run.

The Department for Courts reporting to me on this information matching programme showed promise of being both thorough and automated. Unfortunately "teething problems" are continuing to show up and my staff will continue to work with the Department to improve the accuracy and timeliness of these reports.

Totalling the three runs for which twelve-month reports have now been completed (two actually run last year, and one this year), a clear pattern emerges. Of 110,356 names sent to DWI for matching, 19,465 produced "raw hits" or apparent matches. Of these, 114 were not useable addresses, and 7,808 turned out to have been in contact or otherwise cleared up before Courts had acted on the information matching results. Of the remainder, which gave useable addresses for individuals with whom the Department had not already made recent contact, 2,371 were successfully challenged by the addressee after receiving a s.103 notice (predominantly because the addressee could show that they were not the individual being sought) and just 9,059 individuals had some collection process instituted with the assistance of this information matching programme. These 9,059 cases involved a total outstanding debt of $6,436,112.

TABLE 20: DWI/COURTS FINES DEFAULTERS ADDRESS MATCH – 1999/2000 RESULTS (BY RUN DATE)

Run date	6/99	9/99	11/99	1/00	3/00	4/00
Names sent for matching	43,176	50,000	45,611	45,161	No reports received yet	No reports received yet
Names matched	6,413	12,596	10,151	7,650		
Useable matches	6,395	12,596	10,071	7,616		
Cleared before notice	2,252	3,040	4,622	3,108		
Successfully challenged	781	395	1,326	1,103		
Collection instituted	3,299	9,118*	1,391*	1,424*		

*Note that these figures are not yet final: contacting and collection processes are still being worked upon

Table 20 (previous page) sets out basic statistics for the match runs conducted in 1999/2000, with comparable figures for the last run of the previous year.

I believe that the number of successful challenges, presumably in response to the arrival of a s.103 notice, is a matter meriting concern and further investigation as to the accuracy of the matching process. I will be taking this up with Courts.

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

I. DWI/IRD Family Support Match

DWI/IRD FAMILY SUPPORT MATCH	
Information matching provision	Tax Administration Act 1994, s.84
Year authorised	1993
Commencement date	1995
Match type	Confirmation of continuing eligibility
Unique identifiers	Tax file number
On-line transfers	None

The DWI/IRD Family Support Match[20] is designed to prevent people "double-dipping" by receiving family tax credits from both IRD and DWI. IRD periodically sends records to DWI which carries out the process of comparison. Where there is a positive match, the person's details are referred back to IRD to use the results to take adverse action.

In this programme, IRD is both a "source agency" and "user agency", with DWI being the "matching agency" (i.e. carrying out the automated process of comparison). As a rule of thumb, it is often most convenient for the agency with the smaller number of records to be compared to disclose those records to the agency with the larger database to carry out the process of comparison.

Results

TABLE 21: DWI/IRD FAMILY SUPPORT MATCH – 1997-2000 RESULTS			
	1997/98 Runs 24-32	**1998/99 Runs 33-41**	**1999/00 Runs 42-50**
Cases sent by IRD to DWI for matching	797,230	878,754	935,176
Cases matched by DWI	6,297	6,889	8,019
Cases of adverse action taken	4,927	5,524	6,506
Costs incurred by IRD	$538,017	$460,198	$226,569*
Savings (estimated)[21]	$12,537,265	$14,563,098	$15,055,335
*see comments below regarding costs			

20 Formerly referred to as the "WINZ/IRD Family Support Match", the "NZISS/IRD Child Support Match" or "the Family Support Match". Sometimes referred to by departments as "the Double-Dipping Programme".

21 Calculated by determining the amount of the payments stopped, multiplied by the number of fortnights left in the customer's tax year, ie to the end of March (when the payment ought normally be stopped/ reviewed because of the filing of a tax return).

As can be seen from the statistics in the above table, the volumes and outcomes of this information matching programme show a gradual increase. There were nine runs in this year, each covering about 100,000 individuals.

The figures for "costs incurred" and for "savings estimated" merit some explanation. The substantial reduction in costs for the 1999/2000 year apparently has two causes, one technical and one real. During the year there was a change in IRD's activity coding and cost allocation system which resulted in one quarter's costs showing negative figures to make a retrospective adjustment. The resultant total is not directly comparable with the figures shown for prior years. However, a second reason for cost reduction is a genuine saving which arises from the fact that most data filed by employers is now received electronically, eliminating the need for this information to be keyed in by IRD and thus reducing the costs of preparing data for information matching activities.

The figures for estimated savings in this match are more an indication of cash flow savings rather than real losses avoided. The figures estimate the extra money which would have been paid out (or not collected in) if the "double dipping" had gone on until the end of the tax year. However, the tax calculations at the end of a tax year would always rectify the situation by creating a recoverable debt (or reducing a refund otherwise payable).

The true savings achieved by this programme would depend among other things upon the cost of government borrowing and the costs and delays involved in recovering individual tax debts, but would probably be less than 10% of the figures shown by IRD. Even so, it seems likely that the real monetary savings achieved by the programme comfortably exceed its present level of costs.

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

J. NZIS/EEC Unqualified Electors Match

NZIS/EEC UNQUALIFIED ELECTORS MATCH	
Information matching provision	Electoral Act 1993, s.263A
Year authorised	1995
Commencement date	August 1996
Match type	• Confirmation of eligibility • Detection of illegal behaviour
Unique identifiers	None
On-line transfers	None

The Unqualified Electors 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 also listed as either visitors to New Zealand or overstayers.

Details of any names matched are sent to the Registrar of Electors in the electoral district 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, evidence of citizenship) the person may be deleted from the electoral roll. If there is no reply to the notice, a procedure established in s.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

The programme did not operate last year and operated just once in 1999 prior to that year's general election. The basic timetable was:

- 17 August - initial data received from NZIS;
- 18 August - matching undertaken;

- 19 August - raw hits returned to NZIS for quality check;
- 26 August - final data received from NZIS following confirmation procedures;
- 6 September - s.103 notices of adverse action delivered;
- 13 September - last day to respond to s.103 notices;
- 21/22 September - Electoral Act notices given;
- 7 October - action taken by Registrars of Electors;
- 27 November - General Election.

At my request, the EEC provided a breakdown by visa/permit type for the records sent by NZIS for matching. It needs to be remembered that the match does not simply look for people unlawfully in the country (overstayers) to see if they have enrolled, but also makes a check of the records of visitors lawfully here but not entitled to vote. When the match was first proposed I queried whether it was necessary to match with visitor data since the inclusion of that large group in the match might multiply the error rate without necessarily bringing corresponding benefits in electoral terms. However, I have been willing to suspend judgment pending the results of actual matching.

The breakdown of the 105,997 records supplied by NZIS for matching was:

- visitors - 76,723 names;
- students - 15,340 names;
- workers - 12,748 names;
- overstayers - 1,186 names.

The numbers of overstayer records sent for matching is artificially low in this year's programme since a decision was taken to use only "confirmed" overstayer information. This decision, which I support, was taken because of concerns about the data quality of the overstayer list. These problems were mentioned in my annual reports for the last two years and highlighted in a report by the Auditor-General.[22]

22 *Report of the Controller and Auditor-General: Third Report for 1997*, The Compliance Function of the NZ Immigration Service, p 49.

Table 22 shows a breakdown of the results by immigration status. Although the results are interesting it may be premature to offer any firm conclusions on the differences between the categories as this is the first time with this breakdown. It will be important to follow the trends next time to judge the utility of the match in respect of particular groups of people temporarily in the country.

TABLE 22: NZIS/EEC UNQUALIFIED ELECTORS MATCH – 1999 RESULTS BY IMMIGRATION STATUS

Immigration status	Records matched	Raw hits	Checked hits	Checked "hit rate"
Visitor	76,723	320	65	0.09%
Student	15,340	54	41	0.28%
Worker	12,748	68	54	0.42%
Overstayer	1,186	60	16	1.35%
Totals	**105,997**	**502**	**176**	**0.17%**

The "hit rate", being the number of checked hits divided by the total number of records matched, is fairly low across the match although, as might be expected, the rate for overstayers is significantly higher than for the other groups.

Also of interest is the fact that of the 502 raw hits received only 176 remained after checking. In this regard the match illustrates the importance of post-match confirmation procedures. In this programme the departments have taken steps, through post-match checking and the exclusion of unverified records from the overstayer list, to help ensure that the error rate does not affect excessive numbers of individuals.

Section 103 of the Privacy Act establishes the important safeguard that notice must be given to the individual concerned before any adverse action is taken on the basis of a discrepancy produced by a matching programme. Section 103 notices were given to the 176 electors for whom a checked hit was produced before any action was taken to remove them from the roll. Of the 176 notices sent out, some 15 individuals established that they were indeed New Zealand citizens or permanent residents. Although the absolute numbers are small, this represents 8.5% of the notices sent out which is a significant proportion. Such notices make it plain that individuals are not to be "presumed guilty" at this point and that they have a chance to prevent further processes being initiated.

However, the Privacy Act only requires five working days notice to be given and it is understandable that some people may have missed the opportunity to respond through absence. In the later stages of the process, under the Electoral Act, a further five individuals established their entitlement to remain on the electoral roll by virtue of their citizenship or permanent residence. Of the 20 successful challenges, all but three had been matched from the list of visitors (the remainder being from the list of people on work permits).

TABLE 23: NZIS/EEC UNQUALIFIED ELECTORS MATCH – RESULTS 1996, 1997 and 1999

	1996	1997	1999
Discrepancy/section 103 notices sent	315	86	176
Retained on electoral roll (successful challenge)	30	9	20
Voluntarily removed from roll	72	13	50
Removed from roll or placed on dormant roll (not served or no response)	213	64	106
Costs	*	$7,523	$12,087

*Figure not available

It does seem plain that the absolute numbers of ineligible electors identified is tiny. The proportion of successful challenges (20 out of 176) is also higher than other matches operated currently. The overall cost of the match is modest given the sums expended to maintain the electoral roll and conduct elections. Some might think that the match represents an expensive way to find a fairly small number of ineligible electors who might, in due course, never have voted anyway. Others may well see the small sums expended as being money well spent to offer public assurance as to the reliability of the roll in one particular respect. At present I am willing to suspend judgment on that score but I can say that on the information presented to me, I am of the view that the programme was operated in accordance with ss.99-103 of the Privacy Act and the information matching rules.

K. IRD/Accident Insurance Regulator Employer Compliance Match

IRD/ACCIDENT INSURANCE REGUATOR EMPLOYER COMPLIANCE MATCH	
Information matching provision	Accident Insurance Act 1988, s.370
Year authorised	1998
Commencement date	1999
Match type	• Detection of illegal behaviour • Updating of data
Unique identifiers	• Tax file number • Insurance number
On-line transfers	None

As part of the introduction of privatised workplace accident insurance in mid-1999, an information matching programme was introduced to monitor the entry of every employer into workplace accident insurance cover with one of the seven insurers approved for this purpose. The matching programme compared the details of all employers known to Inland Revenue with the corresponding details of employers taking out workplace accident insurance cover. It was conducted by the Accident Insurance Regulator ("the Regulator"), who was at all relevant times located within the Department of Labour.

All employers were required to have such insurance in place by 1 July 1999, and those who did not expressly arrange insurance policies were allocated to At Work Insurance Ltd ("@Work") which insured them by default and then had to assess, charge and get paid the appropriate premium for that cover. Thus the initial runs of the information matching programme, which took place in May and June of 1999 and were covered in my last annual report, were really designed to produce the list of employers allocated to @Work. The process of compiling and refining that list continued until at least September 1999.

Since 1 July 1999 the Regulator has continued to identify, investigate and, if warranted, take enforcement action against any individuals or companies which become employers after that date. This involves the same kind of information matching programme being run periodically, comparing new employers known to IRD with new employers taking out insurance contracts.

The same information matching and subsequent enforcement procedures are applied to all apparent employers, whether they are individuals or companies. However, the Privacy Act only applies to personal information which is about natural persons, and not at all to information which is about companies. Because the Regulator had no need to distinguish between the two forms of entity, and was prepared to make the entire process comply with the requirements of the Privacy Act, I had agreed that the Regulator's reports to me could give aggregate figures for all employers. It follows that the figures given below are for all employer entities, many of which will be companies and thus not subject to Privacy Act protection in the use of information about them. Had the system continued to operate, I would have asked for some sampling exercises to establish the proportion of employers in the various statistics reported who were "natural persons". As it is, the information matching programme operated by the Regulator has now come to an end as a result of the privatisation process being reversed by the incoming government.

Results

Experience with the initial runs of this information matching programme last year showed many problems with the incoming data which had not been fully anticipated. For different reasons, both the information obtained from IRD and the information obtained from the insurance companies was found to be seriously unreliable for use in the Regulator's operation. For instance, IRD's records did not distinguish between PAYE tax deducted from employee wages and tax withheld from contractor payments. Insurer-supplied information was often late, and not infrequently showed incorrect "AIN" reference numbers (the Accident Insurance Number earlier assigned by the Regulator and upon which the matching operation depended). Largely because of these data problems, the Regulator did not use the information matching programme between July 1999 and January 2000.

Of 29,083 apparent new employer records received from IRD during the 1999-2000 year, 6,899 were initially identified as uninsured because they did not match with any insurer's records. Of these, 2,479 were resolved by internal checking (including late returns by insurers, or entry into insurance contracts during a short period of grace after becoming employers). Notices were sent to 4,420 apparently uninsured employers under s.103 of the Privacy Act, advising them of the apparent discrepancy and giving an opportunity to show why adverse action should not be taken against them. The

notices produced 768 objections (assertions that there was something wrong with the information matching in their case) and a further 3,025 cases in which the apparent employer was able to show that enforcement action would not be appropriate. This left only 627 cases for imposition of a penalty, which involves a second information matching programme that is described later in this report.

Had the process and the information matching programme been continuing, I would have called for more detailed reporting and investigation of the reasons why the large majority (over 85%) of the cases for which a s.103 notice was issued did not eventually warrant any penalty action. As it was, many of the reasons which have been mentioned to me (without statistical breakdown) would have been limited to conditions and misunderstandings surrounding the introduction of the privatised insurance scheme, and should not have occurred in succeeding years. The system never got sufficient chance to "settle down". This information matching programme ceased operating in April 2000.

The Regulator having now ceased operating the information matching programme, I am advised that all information produced by it has been destroyed except for that still needed for enforcement and collection of penalties. I believe that the information matching programme was operated in accordance with ss.99 to 103 of the Privacy Act and with the information matching rules.

The history of this programme illustrates the importance of careful examination and trial runs before operating and relying upon the results of automated processes for the compilation and comparison of information. The programme had to be designed and implemented rapidly to meet a tight timetable set by Parliament for the introduction of the privatisation scheme on 1 July 1999. A good deal of consultation went on between the Regulator's office, IRD and the insurance companies. Nevertheless, when the resulting programme was put into operation it produced types and volumes of errors far beyond what had been anticipated and the results needed much more individual investigation and verification before they could be relied upon at all.

Compliance with the requirements of Part X of the Privacy Act was, I believe, of significant practical value to this match, particularly the use of notices under s.103 which will have defused a lot of potential outrage among individuals and companies being wrongly accused of default in an employer's legal obligation.

L. IRD/Accident Insurance Regulator Sanction Assessment Match

IRD/ACCIDENT INSURANCE REGULATOR SANCTION ASSESSMENT MATCH	
Information matching provision	Accident Insurance Act 1998, s.370
Year authorised	1998
Commencement date	2000
Match type	Updating of data
Unique identifiers	Tax file number
On-line transfers	None

The second information matching programme operated by the Accident Insurance Regulator involved the Regulator sending to IRD certain details of employers against whom adverse (penalty) action was being taken. Inland Revenue matched those details against their own records and reported back to the Regulator on the employment payroll value and the industry classification of each employer concerned. This information was then used by the Regulator to fix a notional insurance premium and then a penalty sum payable by the employer.

This penalty-assessment information matching programme was used by the Regulator from January to April 2000. There were 627 penalties assessed, being the number of non-compliance penalty cases confirmed by individual investigations following on from the initial information matching programme discrepancies discussed above. The total of penalties assessed and imposed was $621,255, with a median penalty value of $575. At the time of the Regulator's final report to me, no data was available on any challenges to the assessment process or calculations, or on the collection of penalty sums.

I have no reason to believe that the programme was not carried out in accordance with ss.99-103 of the Privacy Act and the information matching rules.

Matches which did not operate during the year

M. IRD/Courts Fines Defaulters Address Match

IRD/COURTS FINES DEFAULTERS ADDRESS MATCH	
Information matching provision	Tax Administration Act 1994, s.85A
Year authorised	1998
Commencement date	Not yet commenced
Match type	Location of persons
Unique identifiers	None
On-line transfers	None

Under the IRD/Courts Fines Defaulters Address Match, the Department for Courts is to be supplied by IRD with address and telephone information concerning those fines defaulters for whom IRD has details. The purpose of the programme is to locate those who owe fines in order to enable recovery of outstanding amounts. The programme is intended to complement the address match with DWI since that other programme is more likely to reveal contact details for persons outside the workforce (that is, receiving income support), whereas IRD's records are likely to be better in relation to people in employment who are paying tax. This programme has not yet commenced.

N. Corrections/ACC Inmates Match

CORRECTIONS/ACC INMATES MATCH	
Information matching provision	Accident Insurance Act 1998, s.353
Year authorised	1992
Commencement date	Not yet commenced
Match type	Confirmation of continuing eligibility
Unique identifiers	None
On-line transfers	None

The purpose of the Corrections/ACC Inmates Match[23] is to enforce the provision, now contained in s.122 of the Accident Insurance Act 1998, which disentitles inmates from receiving accident compensation during imprisonment. It would do this by having the Department of Corrections disclose inmate details to ACC for comparison with the records of people receiving accident compensation.

In the last week of the previous financial year an information matching agreement was signed between ACC and the Department of Corrections providing for this match. However, the programme did not operate during the year. I am advised that discussions between the departments continued on a number of matters preliminary to getting the match started.

In last year's annual report, I mentioned a matter that my office had raised about the addressing of notices of adverse action in the Corrections/DWI Inmates Match. The issue was that a notice solely sent to a prison provides no safeguard in the event of records having been wrongly matched. I am pleased to note that ACC has indicated that when the match begins it intends to employ the dual notification approach suggested by my office. This would mean that notices would be sent to the individual at the most current address held on ACC's records with a copy of the notice also addressed to the named individual at the prison. This should ensure that the individual would receive the notice one way or the other. ACC is also considering the option of applying to Corrections to have its freephone number approved for inmate use so that individuals could respond to the notice by telephone.

23 Formerly referred to as the "Corrections/ACC Match".

O. ACC/IRD Child Tax Credit Match

ACC/IRD CHILD TAX CREDIT MATCH	
Information matching provision	Tax Administration Act 1994, s.46A
Year authorised	1996
Commencement date	Not yet commenced
Match type	Confirmation of eligibility
Unique identifiers	Tax file number
On-line transfers	None

The law authorising the ACC/IRD Child Tax Credit Match[24] seeks to facilitate the exchange of information between ACC and IRD for the purpose of verifying entitlement to the Child Tax Credit (formerly the Independent Family Tax Credit). Section 46A of the Tax Administration Act provides that ACC must provide, on request from IRD, in respect of each person receiving weekly compensation continuously for three months or more, that person's name and address, tax file number, and date of birth and the periods for which the person has been receiving weekly compensation for three months or more. The section further empowers IRD to compare the information with IRD information in order to assess that person's entitlement or their spouse's entitlement to the tax credit.

No information matching agreement has yet been entered into in relation to this match. The programme has not yet begun and advice from IRD is that there is "little likelihood" of the programme being implemented "in the short term".

24 This programme was formerly referred to as the "ACC/IRD Independent Family Tax Credit Match".

P. IRD/ACC Earners Match

IRD/ACC EARNERS MATCH	
Information matching provision	Tax Administration Act 1994, s.82
Year authorised	1991
Commencement date	1997 (operation subsequently suspended)
Match type	• Confirmation of continuing eligibility • Detection of illegal behaviour
Unique identifiers	Tax file number
On-line transfers	None

The purpose of this programme is to detect individuals fraudulently receiving ACC compensation while also receiving other undeclared income. As reported in previous annual reports, a test run of this programme was carried out some years ago but the programme did not become fully operational as some fundamental problems in the match needed to be resolved. IRD indicated to me in its report to the end of June 2000 that it had been expected to have progressed the development of this programme with ACC by that date. However, with various legislative changes and competing priorities over the preceding period there had been some slippage in development. I was advised that it is now expected that this programme will commence operating in the latter half of 2000.

Q. NZIS/DWI Immigration Match

NZIS/DWI IMMIGRATION MATCH	
Information matching provision	Immigration Act 1987, s.141A
Year authorised	1991
Commencement date	Not yet commenced
Match type	• Detection of illegal behaviour • Confirmation of continuing eligibility
Unique identifiers	None
On-line transfers	None

The NZIS/DWI Immigration Match[25] anticipates the Department of Labour, which in this context will mean the NZ Immigration Service, disclosing information to DWI about people believed to be unlawfully in New Zealand, or lawfully here only by virtue of being on a temporary or limited purpose permit, in order to verify entitlement to a benefit or the amount of a benefit.

Although the programme was authorised nine years ago it has never operated. DWI advised that during the year it "has not been progressed, nor is it likely to in the near future".

25 This programme was referred to in last year's annual report as the "Labour/WINZ Immigration Match."

V. Financial and Performance Statements for the Year Ended 30 June 2000

CONTENTS

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 judgments 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 2000.

B H Slane
PRIVACY COMMISSIONER

Privacy Commissioner Statement of Accounting Policies for the Year Ended 30 June 2000

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.

MEASUREMENT SYSTEM

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.

ACCOUNTING POLICIES

The following accounting policies, which materially affect the measurement of the financial performance and the financial position on an historical cost basis, have been followed.

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 for the preparation of the financial statements.

Revenue

The Privacy Commissioner derives revenue from the provision of services to Parliament, for services to third parties and inter-

est on its deposits. Such revenue is recognised when earned and reported in the financial period to which it relates.

Debtors

Debtors are stated at their estimated realisable value, after providing for doubtful debts.

Leases

Operating lease payments, where the lessors 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.

Fixed assets

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

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
Computer Equipment	4 Years

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.

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.

Goods and Services Tax (GST)

All items in the financial statements are exclusive of GST. With the exception of accounts receivable and accounts payable which are stated with GST included. Where GST is irrecoverable as an input tax, it is recognised as part of the related asset or expense.

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.

Contingent liabilities

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

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.

Taxation

The Privacy Commissioner is a public authority in terms of the Income Tax Act 1994 and consequently is exempt from income tax.

CHANGES IN ACCOUNTING POLICIES

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

STATEMENT OF FINANCIAL PERFORMANCE FOR THE YEAR ENDED 30 JUNE 2000

1998/99 Actual $		Note	1999/2000 Actual $	1999/2000 Budget $
	INCOME			
1,764,444	Operating Grant		1,864,889	1,864,888
–	Foreign Affairs Grant		28,754	28,754
146,198	Other Income		150,437	121,200
9,661	Interest		21,248	15,000
–	Fixed Asset Adjustment	2	35,735	–
1,920,303	**TOTAL INCOME**		**2,101,063**	**2,029,842**
	EXPENSES			
59,146	Review of the Privacy Act		–	–
65,609	Marketing/Newsletter		74,229	116,400
7,000	Audit Fees		6,500	7,000
65,524	Depreciation		66,758	96,000
210,787	Rental Expense		231,680	216,132
438,137	Operating expenses		454,218	443,722
1,013,270	Staff Expenses		1,155,466	1,153,442
1,859,473	**TOTAL EXPENSES**		**1,988,851**	**2,032,696**
60,830	**NET OPERATING (DEFICIT)/SURPLUS**		**112,212**	**(2,854)**

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

STATEMENT OF MOVEMENT IN EQUITY FOR THE YEAR ENDED 30 JUNE 2000

1998/99 Actual $		1999/2000 Actual $	1999/2000 Budget $
(50,192)	Public Equity at 1 July 1999	191,638	191,638
60,830	Excess of Income over Expenses for the year	112,212	(2,854)
181,000	Capital Injection	–	–
241,830	**Total recognised Revenue and Expenses for the year**	**112,212**	**(2,854)**
191,638	**Public Equity at 30 June 2000**	**303,850**	**188,784**

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

STATEMENT OF FINANCIAL POSITION AS AT 30 JUNE 2000

1998/99 Actual $		Note	1999/2000 Actual $	1999/2000 Budget $
10,638	Surplus from operations		303,850	188,784
181,000	Capital Injection		–	–
191,638	**PUBLIC EQUITY**		**303,850**	**188,784**
	Represented by:			
	ASSETS			
	Current Assets			
450	Cash on Hand		450	450
253,637	National Bank		216,136	125,087
23,842	Debtors		7,300	23,842
29,678	Inventory		23,480	29,678
8,001	Prepayments		10,238	8,001
315,608	***Total Current Assets***		**257,604**	**187,058**
31,479	***Fixed Assets***	**2**	**193,164**	**116,479**
347,087	**Total Assets**		**450,768**	**303,537**
	LIABILITIES			
	Current Liabilities			
155,449	Sundry Creditors	1	146,918	114,753
155,449	***Total Current Liabilities***		**146,918**	**114,753**
191,638	**NET ASSETS**		**303,850**	**188,784**

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

STATEMENT OF CASH FLOWS FOR THE YEAR ENDED 30 JUNE 2000

1998/99 Actual $		1999/2000 Actual $	1999/2000 Budget $
	CASH FLOWS FROM OPERATING ACTIVITIES:		
	Cash was provided from:		
1,764,444	Government Grant	1,864,889	1,864,888
137,167	Other Income	195,733	149,954
9,661	Interest	21,248	15,000
1,911,272		**2,081,870**	**2,029,842**
	Cash was applied to:		
812,221	Payments to Suppliers	740,707	788,042
1,060,960	Payments to Employees	1,147,030	1,135,848
10,127	Payments of GST	38,926	53,502
1,883,308		**1,926,663**	**1,977,392**
27,964	**Net Cash Flows applied to operating activities**	**155,207**	**52,450**
	CASH FLOWS FROM INVESTING ACTIVITIES		
	Cash was applied to:		
9,057	Purchase of Fixed Assets	192,708	181,000
(9,057)	**Net Cash Flows applied to Investing Activities**	**(192,708)**	**(181,000)**
	CASH FLOWS FROM FINANCING ACTIVITIES		
	Cash was provided from:		
181,000	Capital Injection	–	–
181,000	**Net Cash Flows applied to Financing Activities**	**–**	**–**
199,907	Net decrease in cash held	(37,501)	(128,550)
54,180	Plus opening cash	254,087	254,087
254,087	**Closing Cash Balance**	**216,586**	**125,537**
450	Cash on Hand	450	450
33,335	National Bank	27,098	25,087
220,302	National Bank – Deposit	189,038	100,000
254,087	**Closing Cash Balance**	**216,586**	**125,537**

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

RECONCILIATION OF NET SURPLUS FROM OPERATIONS WITH THE NET CASH FLOWS FROM OPERATING ACTIVITIES FOR THE YEAR ENDED 30 JUNE 2000

1998/99 Actual $		1999/2000 Actual $	1999/2000 Budget $
60,830	Net surplus/ (deficit) from operations	112,212	(2,854)
	Add (less) non-cash Item:		
65,524	Depreciation	66,758	96,000
–	Fixed Asset Adjustment	(35,735)	–
65,524	**Total non-cash items**	**31,023**	**96,000**
	Add (less) movements in working capital items:		
(78,126)	Increase (Decrease) in Creditors	(8,531)	(40,696)
(2,343)	(Increase) Decrease in Prepayments	(2,237)	–
(8,890)	(Increase) Decrease in inventory	6,198	–
(9,031)	(Increase) Decrease in Debtors	16,542	–
(98,390)		**11,972**	**(40,696)**
27,964	**Net Cash Flows from Operations**	**155,207**	**52,450**

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

STATEMENT OF COMMITMENTS AS AT 30 JUNE 2000

	2000 $	1999 $
Capital Commitments approved and contracted	**–**	**–**
Non-cancellable operating lease commitments, payable:		
Less than one year	206,500	211,606
one - two years	62,500	213,611
two - five years	20,834	83,333
greater than five years	–	–
	289,834	**508,550**

Other non-cancellable contracts:
At balance date the Privacy Commissioner had not entered into any non-cancellable contracts.

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

STATEMENT OF CONTINGENT LIABILITIES AS AT 30 JUNE 2000

There is one known contingent liability of $10,000 as at 30 June 2000. There were no other contingent liabilities as at 30 June 2000.

NOTES TO THE FINANCIAL STATEMENTS FOR THE YEAR ENDED 30 JUNE 2000

Note 1: SUNDRY CREDITORS

1998/99 $		1999/2000 $
45,006	Accruals - Wages and Holiday pay	52,719
23,998	Trade Creditors	23,199
28,190	Accruals	51,671
58,255	GST	19,329
155,449	**TOTAL SUNDRY CREDITORS**	**146,918**

Note 2: FIXED ASSETS

	1998/99 Cost/$	Accum Depn/$	Closing Bk Val/$	1999/2000 Cost/$	Accum Depn/$	Closing Bk Val/$
Office Equipment	279,743	255,900	23,843	160,394	126,837	33,557
Furniture & Fittings	48,038	47,529	509	52,645	49,975	2,670
Computer Equipment	7,127		7,127	320,588	163,651	156,937
	334,908	**303,429**	**31,479**	**533,627**	**340,463**	**193,164**

During the year a stocktake of fixed assets was undertaken and reconciled to the fixed assets register and the general ledger. An amount of $35,735 was recognised in the Statement of Financial Performance as a one off Fixed Asset Adjustment.

Note 3: 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.

3.1 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 2000 is: -

1998/99 $		1999/2000 $
253,637	Bank Balances	216,136
13,347	Debtors	7,300
266,984		**223,436**

Note 4: EMPLOYEES' REMUNERATION

The Commissioner's remuneration and benefits is $169,336 (in 1999 $160,770)

The Commissioner has been requested to implement a Cabinet decision seeking Crown enties to disclose certain remuneration information in their annual reports.

Remuneration of Commissioners and Staff over $100,000 pa

Total Remuneration pa	Number
$160,000 - $180,000	2
$140,000 - $160,000	1
$120,000 - $140,000	2

The Human Rights Commission, the Race Relations Office and the Office of the Privacy Commissioner have combined to produce the above table, which is in $20,000 bands to preserve the privacy of individuals.

Note 5: RELATED PARTY INFORMATION

The Office of the Privacy Commissioner is a wholly owned entity of the Crown. The government is the major source of revenue.

The Commissioner has entered into a number of transactions with (government departments/Crown agencies/state-owned enterprises) where those parties are only acting in the course of the normal dealings with the Office of the Privacy Commissioner. These transactions are not considered to be related party transactions.

During the year the Commissioner purchased services from other related parties not in excess of $800 in total. There were no other related party transactions.

STATEMENT OF OBJECTIVES, STATEMENT OF PERFORMANCE FOR THE YEAR ENDED 30 JUNE 2000

Output - operations of the Privacy Commissioner

	2000 $	1999 $
Total cost of producing output	**$1,988,851**	**$1,859,473**

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. However, the EDS Information Privacy Code 1997 was due to expire on 30 June 2000 and during the year a review of that code was undertaken and an amendment issued to extend its operation to 30 June 2003.

- No application was submitted under section 47(2) for a code to be issued by the Commissioner.

- Two amendments were made to the Health Information Privacy Code 1994.

- Work was reinitiated on proposals for codes of practice in relation to telecommunications and credit reporting and preliminary work, including some industry consultation, was undertaken.

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 1,115 complaints.

- Number of consultations.

Actual Achievement

	Projected	Actual
number of complaints received	1,115	798
number of complaints processed	846	956

- 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 798 complaints were received, jurisdiction assessed and accepted for investigation. Over the same period 956 complaints were resolved or action upon them discontinued and the files closed. Eight commissioner initiated investigations were undertaken.

- During the year 52 formal 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	6,000	5,830

- 5,803 enquiries were formally logged. Of these 5,232 telephone enquiries were answered. 571 written enquiries were received and dealt with during the year. A number of email enquiries and are included in the figures for written enquiries. 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 people on the office mailing lists. The average print run is 5,500 copies.

- The first edition of *On the Record: A Practical Guide to Health Information Privacy* was published.

- A major republication of the Health Information Privacy Code 1994 was undertaken including a rewriting of the extensive explanatory commentary. The new edition was published in June 2000.

- Two general compilations of material were issued comprising papers, submissions and speeches.

- The website was maintained at least fortnightly.

- Eleven case notes were published on the Commissioner's investigations.

- Fifty-six seminars and workshops, and ten speeches were presented during the year by qualified and experienced staff of the office.

- All media statements and the majority of public speeches were made by the Privacy Commissioner personally. The Commissioner received 174 requests by the media that were recorded. Other requests are received and not formally recorded.

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 1999/2000 is contained in this annual report.
- Work continued on the review of a second batch of information matching provisions. The reviews were not completed during the year but is intended to file a report in the second half of 2000.

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 2000

We have audited the financial statements on pages 116 to 133. The financial statements provide information about the past financial and service performance of the Privacy Commissioner and its financial position as at 30 June 2000. This information is stated in accordance with the accounting policies set out on pages 116 to 118.

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 2000, the results of its operations and cash flows and the service performance achievements for the year ended 30 June 2000.

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 Privacy Commissioner in the preparation of the financial statements *and*
- whether the accounting policies are appropriate to Privacy Commissioner's circumstances, consistently applied and adequately disclosed.

We conducted our audit in accordance with generally accepted auditing standards, including the Auditing Standards issued by the Institute of Chartered Accountants of 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 116 to 133:

- comply with generally accepted accounting practice *and*
- fairly reflect:
- the financial position as at 30 June 2000
- 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 27 October 2000 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

Notes