Privacy Commissioner
Te Mana Matapono Matatapu

Report of the Privacy Commissioner

for the year ended 30 June 2001

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

Letter to Minister

November 2001

Minister of Justice
WELLINGTON

I tender my report as Privacy Commissioner for the year ended 30 June 2001.

B H Slane
Privacy Commissioner

Contents

Tables and Figures

Complaints

Enquiries

Functions Under Other Enactments

Information Matching

Figures

I. Introduction

Dispute resolution

One test of the success of a dispute resolution service is the number of matters that are brought to conclusion by mutual agreement. Another test is the number of cases where the complainant has either settled or has decided not to take the matter any further.

In disputes under the Privacy Act (including reviews of access requests which are not always truly disputes) the latter test is whether or not the matter proceeds to the Complaints Review Tribunal.

I am happy to report that only 3.5% of complainants chose to take matters on to the Complaints Review Tribunal. A success rate of 96.5% brings credit, not only to complainants and respondents, but also to the qualities of my investigating staff who bring skills of conciliation and mediation to their work.

A small proportion of complainants will wish to test their case in an open adversarial hearing. They will have their "day in court". I regret to report that once again the Complaints Review Tribunal's concentration on peremptorily disposing of cases - as distinct from hearing them - has resulted in nearly half the cases filed with the Tribunal being struck out without a hearing.

I do not consider that the Tribunal, in dealing with civil litigation, should take an early view that a matter has no merit. Rather, it should proceed to hear cases unless there has been a successful request by a respondent for a matter to be struck out. Nearly all the cases struck out were taken by complainants who were not legally represented.

During the year, on an appeal from the Tribunal, the High Court found the Tribunal had proceeded on a wrong basis in denying damages to a requester in circumstances where a hospital had withheld documents it should have made available to the requester. The High Court commented:

> *This … is the clearest possible example of a Tribunal allowing itself to be improperly influenced by irrelevant matters, and as such is a classic case of proceeding on a wrong principle. On its own, … it would justify interfering with the exercise of the Tribunal's discretion.*

During the year the Government conducted a review of human rights institutions and accepted a recommendation of independent advisers that the Privacy Commissioner's office should not be combined with the offices of the Race Relations Conciliator and the Human Rights Commission. In the course of that review a recommendation has been put to the Government to upgrade the Complaints Review Tribunal. I support that recommendation.

Two of the three members who comprise a Tribunal are drawn from a panel appointed for the purpose. There are vacancies on the panel. As a very high proportion of cases heard by the Tribunal are proceedings under the Privacy Act, I have recommended to the Minister that appointments be made of members whose qualifications and experience particularly suits them for privacy cases. As far as I am aware, all existing appointments have been made with the Human Rights Act jurisdiction in mind.

It is important that the Tribunal have the stature to deal with human rights, privacy and health and disability cases in an authoritative way and give decisions which set valuable precedents for subsequent cases. This is more important than disposing of business quickly. Many people with unresolved grievances warrant, if not a day in court, an hour or so to explain their case and to be satisfied that their case has been understood at a hearing.

This is particularly the case when due to the stretched resources of the office I have taken the trouble to recommend to some parties that they may get an earlier and more satisfactory resolution by going directly to the Tribunal. Regrettably, some who did that found they ended up with neither an investigation by the Privacy Commissioner nor a hearing by the Tribunal.

International

The international data protection privacy scene has been distinguished by the efforts made by the United States, Australia and Canada to secure recognition by the European Union of the privacy regimes in their country. They would be regarded as "adequate" to receive the transfer of personal data from European countries in accordance with a European Directive on transborder data flows.

It is interesting to observe that Canada, which started 8 years behind New Zealand with coverage of the private sector, has al-

ready secured a place ahead of New Zealand in the queue for consideration. Australia has put the resources of its Attorney General's department behind achieving recognition and has engaged the European Union in a significant debate on the EU's attitude to Australia's new privacy law which is yet to come into force.

By contrast New Zealand governments have taken little interest until recently in securing a recognition of adequacy for New Zealand law. The indicator of this is the time it has taken to bring about two changes in the Privacy Act which are seen as being essential to any negotiation with the European Commission.

This can be contrasted with the public espousal by all governments of the need to compete internationally, to assist exporters, to encourage those who provide services to foreign countries and to participate actively in electronic commerce.

I have to say it has been my office that has driven the activity that has been achieved and has conducted preliminary negotiations with the European Commission. Two amendments to the Privacy Act were promoted first in 1998. They were eventually introduced into Parliament in a Statutes Amendment Bill this year by agreement with all parties.

Subsequently one party withdrew its support of one amendment and so it can no longer remain in the Statutes Amendment Bill. Its future seems precarious. I hope that those responsible for the business of the House of Representatives will ensure that whatever vehicle these amendments proceed in is given priority. Before long it may be possible to place New Zealand in an advantageous position compared to other countries. We have a good privacy law and although it is not identical to the data protection laws in Europe, I believe it provides adequate protection for European data coming to New Zealand. With the amendments recommended, we have a reasonable chance it ought to receive approval from the EU. It will probably take at least another year to pass through the European necessary processes.

The standing in which New Zealand is held internationally, both for the work of this office and for the Privacy Act and the Health Information Privacy Code, bear witness to the groundwork done by the New Zealand legislature on the Privacy Act. It also recognises that New Zealand is part of the modern world and leads the way for many other countries. Our Privacy Act has been used as an exam-

ple for other countries and parts of our Health Information Privacy Code have found their way into the law of other jurisdictions.

I am pleased to announce that the International Working Group on Data Protection in Telecommunications has accepted our offer to host a meeting in Auckland in March 2002. This prestigious group, created by the International Conference of Data Protection and Privacy Commissioners, is at the forefront of privacy concerns in new technologies. It produces position papers which set standards for law and action in many countries. I am pleased to have been able to arrange, in conjunction with that meeting, for the 3rd Asia Pacific Forum to be held in New Zealand. It is the first to have been hosted outside Hong Kong. I will take advantage of the presence in New Zealand of information commissioners from other jurisdictions to have a one-day symposium on freedom of information and privacy.

During the year, New Zealand was honoured to be included in a committee established by the 23rd International Conference of Data Protection and Privacy Commissioners to establish procedures and a basis for accrediting data protection and privacy authorities to attend and vote at the International Conference. Together with France and the United Kingdom, we prepared reports for consideration at the 24th meeting in September 2001. The adoption of these recommendations will establish some basic standards for such authorities.

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 had 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, case notes, 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.

STAFF

At 30 June 2001 the following staff were employed in the Auckland and Wellington offices.

Susan Allison	Librarian (part-time)
Victoria Anderson	Investigating Officer
Marilyn Andrew	Support staff (part-time)
Phillipa Ballard	Manager, Investigations
John Blakeley	Data Matching Compliance Officer
Brent Carey	Investigating Officer
Katy Cook	Investigating Officer
Eleanor Cooley	Support staff
Bernard Darby	Privacy Policy Officer (part-time)
Terry Debenham	Enquiries Officer
Ina de Polo	Support staff
Michael des Tombe	Investigating Officer
Michelle Donovan	Legal Officer Investigations
Antonia Dowgray	Investigating Officer
Godfrey Eagar	Investigating Officer
Annabel Fordham	Executive Officer
Margaret Gibbons	Support staff
Fred Henderson	Enquiries Officer
Eve Larsen	Support staff
Sharyn Leonard	Support staff (part-time)
Tania Makani	Complaints Management Officer
Sebastian Morgan-Lynch	Investigating Officer

Sharon Newton	Support staff
Glenda Osborne	Accounts Clerk (part-time)
Kimberley Parkin	Investigating Officer
Carolyn Richardson	Investigating Officer
Jacci Setefano	Investigating Officer (part-time)
Amir Shrestha	Support staff
Blair Stewart	Assistant Commissioner
Wayne Wilson	Legal and Policy Adviser

I have also been well served by **Gary Bulog**, **Robert Stevens**, **Graham Wear**, **Rachel Bruce**, and **Shane Clapson** who have been variously involved in management, legal, advising, accounting and publication projects for me. During the year **Deborah Marshall**, Manager, Investigations and **Kristin Langdon**, Deputy Manager Investigations, left to pursue legal careers. Their contribution to the Office over a number of years has been significant and is greatly appreciated.

III. Report on Activities

CODES OF PRACTICE

Introduction

One important feature of the scheme of the Privacy Act is provision for codes of practice. Codes provide a mechanism whereby the rules for information handling can be modified and applied in particular circumstances. Under Part VI of the Privacy Act, I may issue codes in relation to agencies, information, activities, industries, professions and callings. Codes may also be issued under Part VII in relation to public registers.

A code issued under the Act can modify the application of the information privacy principles by prescribing standards that vary from those prescribed by the information privacy principles or by exempting particular actions from the principles. A code may also prescribe how the principles are to be applied or complied with. Codes can do various other things, such as regulating information matching in the private sector, setting guidelines in relation to charging for access to information and prescribing procedures for complaints handling.

The Act sets down requirements that must be followed before I may issue a code of practice. I am required to do everything reasonably possible to advise persons who may be affected by the proposed code, or their representatives, of the proposed terms of the code and the reasons for it, and to seek their views. I am also obliged to give public notice of my intention to issue a code and invite public submissions. I usually create a mailing list of persons who may be interested and ensure that they receive details of the proposal and include messages in *Private Word* and on my website. I also work with relevant industry groups or government departments who can disseminate a message more widely within their industry or sector or the community generally. Often I go further than the statutory requirements and seek out the views of interested persons *before* publicly notifying a proposal for a code (as has been the case this year in the areas of telecommunications and credit reporting).

Codes of practice issued by the Privacy Commissioner have the status of regulations for the purposes of the Regulations (Disallowance) Act 1989. This means that they are tabled in Parliament and

are the subject of routine scrutiny by the Regulations Review Committee. Anyone who is dissatisfied with a code, or a provision in a code, can complain to the Committee and Parliament has the power to disallow a code of practice. Scrutiny by the Regulations Review Committee, provision for complaint and the power to disallow a code combine to provide powerful safeguards.

I issued no new codes of practice during the year. Nor did I amend any existing code. The following codes, 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.

Post-Compulsory Education Unique Identifier Code 2001

The Ministry of Education approached me in May 2000 in relation to a proposed national student index project. The proposal raised a number of information privacy issues but the Ministry's principal compliance difficulty related to its plan to create a sector-wide unique identifier for tertiary students and to use this in relation to a proposed data warehouse. This aspect of the proposal could not be reconciled with information privacy principle 12(2) which prohibits agencies from assigning a unique identifier that has already been assigned by another agency. This prohibition is designed to inhibit the creation of common numbering systems, such as a national ID number, with the significant privacy risks associated with such systems.

My office worked through the issues with the Ministry and examined the objective of the proposal, the uses to which the number would be put, and the possibility of an alternative way of achieving the objective. The Ministry was asked to study the issues carefully and to document its position: it did this in a privacy impact assessment (PIA) which it submitted to me in October. Following further discussion with my office the PIA was reworked and a revised version provided in January 2001. I wrote to the Secretary of Education confirming that I had studied the PIA and was inclined to agree to the Ministry's request that I move towards issuing a code of prac-

tice. Depending upon the results of public consultation, I would decide whether finally to issue the code.

While the key legal effect of the code would be to provide an exemption from principle 12(2), that alone would not adequately address the privacy issues. The principal objective of the programme was to enable statistics to be generated on educational issues. It was not intended to create a general administrative number for students for all purposes. Considerable care was therefore needed in preparing the code and that process took several months, involving both the Ministry and my office. To address the totality of the issues the code dealt not only with controls on the uses of the proposed student index number, but also with the associated data warehouse.

I publicly notified my intention to issue the code of practice in April. More than 150 copies of the proposed code were mailed to organisations in the education sector and to other interested people. Details were also given in *Private Word* and on my website. The Ministry's PIA was also made available on my website.

The code had not been issued at the end of the financial year. However, the code was issued shortly thereafter on 14 August. Some minor changes were made as a result of the submissions received.

Telecommunications and credit reporting

As reported in my previous annual report, I recommenced work in 2000 on two longstanding proposals for codes of practice in the area of credit reporting and telecommunications.

Last year I commissioned a resource document by Nigel Waters, a privacy expert from Australia. There has been considerable interest in *Privacy on the Line: A Resource Document in relation to Privacy in Telecommunications* and many copies have been distributed free of charge by my office and from my website. I brought Nigel Waters to New Zealand to give presentations on telecommunications privacy issues to the privacy forums held in Auckland and Wellington in July 2000.

Neither code reached the stage where I publicly notified my intention to issue it. Instead, my staff have been seeking stakeholder views on the proposals and, in particular, considering industry comment on draft versions of the proposed codes. This work has taken

longer than anticipated, but many of the issues are complicated and the prolonged study will contribute to better final codes. My office released draft versions of both codes in June 2001 to the wider public. This generated some media coverage and attracted the attention of some further industry players as well as interested individuals.

I intend to publicly notify both codes before the end of 2001. This will enable public participation in the process before any final decisions are taken.

COMPLAINTS

While the number of complaints closed in this financial year is less than in some previous years, there were almost 90 more complaints received this year than last year. I have previously expressed a view that the number appeared to be declining. I believed this reflected the fact that complainants may be reluctant to embark on the process, given that there is a significant delay between the time a complaint is received and when it is assigned to an investigating officer. However, the increase in complaint numbers this year would seem to suggest that the delay is not a serious impediment to complainants. Most complainants appear to be aware that it could be some time before their complaint is dealt with by an investigating officer and are prepared to wait the requisite time, apparently satisfied that a thorough investigation will eventually ensue.

The number of complaints received was relatively steady throughout the year, but there was a marked increase during the month of May and early June, which coincided with a series on privacy published in the *New Zealand Herald*. Table 1 represents the number of complaints received and disposed of during the financial year.

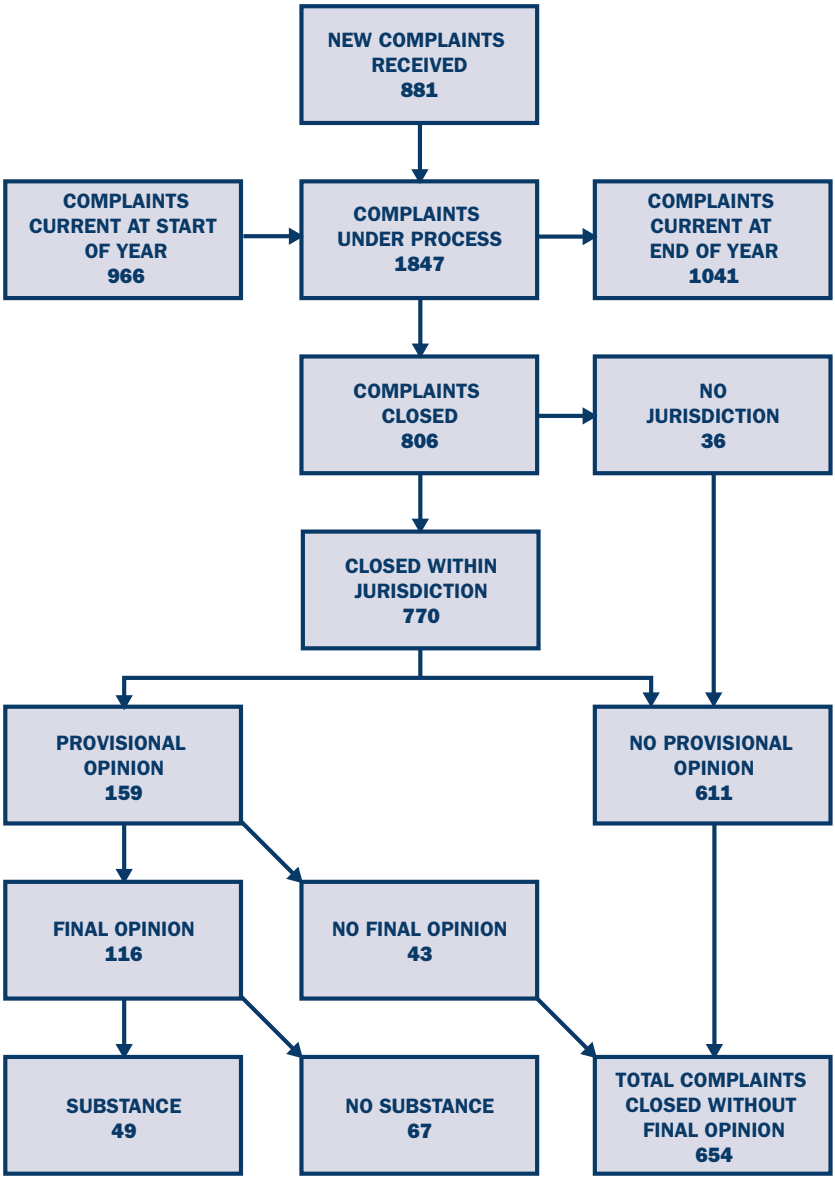
TABLE 1: COMPLAINTS RECEIVED AND CLOSED 1995-2001

	1995/96	1996/97	1997/98	1998/99	1999/00	2000/01
Complaints received	993	1200	1088	1003	798	881
Complaints closed	972	870	804	895	956	806

Refer Figure 1 (page 21).

There were 881 new complaints received during the year and 806 complaint files were closed. Of those, 402 complaints were closed while in the queue and 404 were closed after investigation. At the end of June, 1041 complaints were current, including 750 which were in the process of investigation, and 291 which were in the queue prior to being assigned to an investigating officer. This is lower than the 623 in the queue at the end of the last financial year, and lower than the high point of just over 800 during May 2001. As a result, the time between when a complaint is received and when it is assigned to an investigating officer has dropped from 18 months on average to about 12 months.

FIGURE 1: COMPLAINTS 2000/01



The concept of a queue of complaint files implies that once received and acknowledged, the files remain dormant for a number of months. This is far from the case. A Complaints Management Officer, assisted by the Complaints Team Leader and Manager Investigations, communicated with queue complainants eliciting further information, clarifying issues and encouraging complainants and respondents to consider means by which the complaint might be settled. By this process, during the year 402 complaints were closed before needing an investigating officer. Other complaints were closed because they were outside my jurisdiction. These included some that were concerned with the personal affairs of the respondents and were excluded from my jurisdiction because of s.56 of the Privacy Act, and some that were referred to the Health and Disability Commissioner and the Ombudsman.

It was possible to resolve 80% of complaints within my jurisdiction without forming a final opinion. These included 43 about which I had formed a provisional opinion but which were settled subsequently, and 575 which had no provisional opinion either because they were settled or because the complainant elected to take no further action. These figures reflect the skills of my investigating staff in assisting the parties to reach a mutually satisfactory settlement.

Dispute resolution captures a major part of my office's resources. During the year I appointed more investigating officers to bring the complement to 10 full time and one part time members of staff. In addition I have a Complaints Management Officer, whose primary task is to manage the complaints and correspond with complainants in the queue. She was assisted by the Complaints Team Leader, and the Manager Investigations when other responsibilities permitted.

Investigation of complaints

Despite the backlog of complaints, almost one third of all complaints are resolved within three months of being received, either because they are settled or because I have formed a final opinion.

The complaints which are not resolved in the queue are generally the more difficult ones, and are eventually assigned to my investigating officers. During the time they have been in the queue, my Complaints Management Officer and Manager Investigations have attempted to assemble as much information as possible so that when they are assigned to an investigating officer some of the

preliminary investigation work has been completed. This is particularly important where complainants, respondents and witnesses are required to recollect incidents – it is certainly preferable to obtain verification of facts soon after the event complained about. However, many complaints still require quite extensive investigation to establish the facts and to clarify the issues. Furthermore, the parties may have become more entrenched in their views after the lengthy wait, and have a reluctance to re-visit issues which they may consider to be somewhat historical.

Section 74 of the Privacy Act provides that where it is possible to secure a settlement between the parties and, if appropriate, an assurance against the repetition of any action which has resulted in the complaint, I should use my best endeavours to secure such a settlement and assurance. During the course of an investigation or while complaints are in the queue, my staff identify those which are amenable to settlement.

Settlement is reached in a number of ways. I invite the parties to propose terms for a settlement, and my staff guide them through a process of negotiation. Often the parties begin far apart, but my staff are able to encourage them to come to a reasonable resolution, guiding them to an outcome which is consistent with other similar complaints. Sometimes, a complainant simply seeks an apology and an assurance that the situation will not be repeated. Agencies which are the subject of such complaints are generally very willing to demonstrate that they have put in place processes which will avoid a recurrence.

Some examples of successful settlements in the past year include:

- A complainant requested access to information which was being relied upon to revoke his visitor's permit. The respondent did not respond within 20 working days and, while some information was eventually supplied, some was withheld for several months. I found that the agency had breached section 40 of the Privacy Act by not responding to the complainant within the statutory time frame. The complainant accepted a payment of $3500 in settlement of the complaint.

- When an employee left his job, he owed the employer money for commissions paid on cancelled insurance policies. The employee began repaying the debt, but disputed the amount owed.

The former employer lodged the debt with a credit reporting agency, and the following month the debt was settled. The employee complained about the debt being listed while discussions regarding the debt were ongoing and about the employer providing inaccurate information about the amount of the debt. I formed the provisional opinion that the employer had breached principle 11 and that it could not rely on the exception in principle 11(a). I also formed the provisional opinion that the employer had breached principle 3 by not informing the employee that it intended to list the debt with a credit reporting agency, and principle 7 because it had not advised the credit agency that the debt had been settled. I found no breach of principle 8. After further correspondence, the employer paid the employee $5000 and the complaint was settled.

- An employee's name was displayed on a white board at one of his employer's offices as being a staff member who was to be made redundant. The information remained on the board for several days and was seen by a number of staff members. Following notification of the complaint, the employer offered the employee $500 to settle the complaint. The offer was accepted and the file was closed without my having to form an opinion.

Complaints involving access

The right of access to one's personal or health information is an important right. As I have observed before, it increases accountability in public and private sector agencies. Once an individual has obtained their personal or health information they have the right to request that information be corrected or, if the agency is unwilling to correct it, to attach a statement of correction to be read in conjunction with the original documents. This helps to ensure that decisions affecting people are based on up-to-date information.

If an individual considers that the agency has not provided them with all of the information which they believe is contained on the file and to which they are entitled, my office can review the agency's decision to withhold some documents. After reviewing the documents that have been withheld, I can recommend either that the agency consider releasing them to the complainant or I will confirm that the grounds under which they were withheld were made out. Some agencies have purported to rely on the ground under section 29(1)(b) of the Privacy Act, which protects the identity of a person who supplied information being evaluative material, apparently unaware

that this section is read in conjunction with section 29(3) which, in part, defines evaluative material as being that compiled for employment and certain other limited purposes.

Of the complaints received this year, 39% included a request for access to either personal or health information or for information under section 22F of the Health Act 1956. As can be seen from Table 2, a greater proportion of access complaints are against public sector agencies.

TABLE 2: COMPLAINTS INVOLVING ACCESS BY SECTOR 1995-2001

	1995/96	1996/97	1997/98	1998/99	1999/00	2000/01
Private sector	176	256	170	148	142	146
Public sector	181	206	179	212	241	201
Total	**357**	**462**	**349**	**360**	**383**	**347**
	1995/96 %	**1996/97 %**	**1997/98 %**	**1998/99 %**	**1999/00 %**	**2000/01 %**
Private sector	49	55	49	41	37	47
Public sector	51	45	51	59	63	53

Some examples of access complaints which have been dealt with this year include:

- A man who belonged to a club was banished from the club after a written complaint was made about his conduct by one of the members. The man requested a copy of the complaint and asked to know the identity of the informant. The club withheld the informant's identity because the informant objected to their identity being known to the man. It was my provisional opinion that the club did not have a proper basis for withholding a complete copy of the letter and that the club's decision to withhold it constituted an interference with the complainant's privacy. The club responded by advising that it considered the complaint had been addressed when the man saw a copy of the letter with the informant's identity deleted. I formed a final opinion that the club's action had caused an interference with the man's privacy, and provided information to the man on how to take the complaint to the Complaints Review Tribunal.

- The complainant requested information relating to her infant son's admission to hospital. Her request was declined on the basis that she had not been named as the child's caregiver and was not the guardian of the child at the time of his admission. She made a second request for the information, pointing out that she was the mother of the child and was therefore entitled to seek and obtain his medical records. She maintained that the fact that she had not been named as his caregiver was irrelevant. This second request was declined on the grounds that the mother was the subject of a restraining order and was therefore not the child's representative. I formed the opinion that even though she was not the child's caregiver, and her guardianship had been removed by the Family Court, as his mother the complainant was his representative. Having established that she was his representative I then considered whether the hospital had grounds for refusing to provide the records. With respect to the first request, I concluded that the hospital had no proper basis to withhold the information as the mother was the child's representative. As for the second request, I formed the view that the existence of a restraining order did not in itself support the hospital's refusal to give her access to the information. In particular I noted that the hospital did not have any legal documentation to support the existence of the restraining order and I was not persuaded that at the time of refusing the complainant's request there was a proper basis for it do so.

Complaints involving disclosure

About 38% of all complaints received are concerned with the disclosure of personal or health information. Principle 11 and rule 11 of the Health Information Privacy Code place limits on the disclosure of information. Disclosure is permitted if an exception to the principle or rule applies - although an agency may decide not to disclose even if an exception applies.

As can be seen from Table 3, there are more complaints against private sector agencies than public sector agencies about unauthorised disclosure of information, although the disparity in numbers is not as great as in previous years. Many disclosure complaints against agencies arise from inadvertent disclosures of information. This demonstrates that my education function remains an important role for my office and that it is necessary to inform agencies of their compliance responsibilities.

TABLE 3: COMPLAINTS INVOLVING DISCLOSURE BY SECTOR 1995-2001						
	1995/96	1996/97	1997/98	1998/99	1999/00	2000/01
Private sector	250	271	195	186	161	185
Public sector	102	100	105	130	103	150
Total	352	371	300	316	264	335
	1995/96 %	1996/97 %	1997/98 %	1998/99 %	1999/00 %	2000/01 %
Private sector	71	73	65	59	61	55
Public sector	29	27	25	41	39	45

Complaints involving disclosure include:

- A life assurance company prepared a sample plan based on one it had prepared for a family. Although some personal information had been omitted from the sample plan, the complainants considered that enough detail remained to identify them to third parties and to employees who received a copy of the plan. After investigation, I formed the provisional view that principle 11(a) did not permit the disclosure of information about the family to the company's employees and others. Following receipt of my provisional opinion, the company agreed to settle the complaint and the complainants were offered $23,000 which they accepted.

- A bank customer opened a savings account and applied for a credit card after separating from her husband with whom she still retained a joint account. In subsequent dealings with the former husband concerning the joint account, his former wife's address was disclosed to him. The parties agreed to settle the complaint and so I was not required to form a provisional opinion. The customer accepted payment of $1500 from the bank and my file was closed.

Other principles

While complaints about access and disclosure constituted the largest number of complaints, I received complaints about breaches of all other principles except for principle 12, which deals with unique identifiers. Alleged breaches of the principles and rules relating to the collection and source of both personal and health information (principles and rules 1, 2 and 3) comprised 15% of total received, and breaches of the principles and rules regarding correc-

tion and accuracy of information comprised just under 10% of total alleged breaches.

Table 4 (page 29) lists all alleged breaches. Some complaints allege a breach of more than one principle, so the total exceeds the total number of complaints received.

Some examples include:

- A complainant alleged that the application for an oil company's promotional card omitted to advise applicants of the possible use to which the information would be put. The complaint raised issues under principles 3 and 5 of the Privacy Act. After investigating the company's procedures, I was satisfied that the company had reasonable safeguards in place to ensure the security of any personal information which it collated. I formed the view that as the applicant was filling in the form voluntarily, they would be aware of the fact that the information was being collected. The company had also advised customers on the form who the intended recipients were, the purpose for which the information was being collected, and their right to have incorrect information corrected. On the basis that there was no interference with the complainant's privacy, I discontinued my investigation of the complaint.

- A gym with a large membership disposed of its members' debit authorisation forms and staff performance files in boxes, which were dumped in a rubbish skip. A member of the public found them in the skip and complained to my office. I investigated the complaint as a breach of principle 5, which provides that an agency shall ensure it protects personal information by such security safeguards as are reasonable. I formed the opinion that the gym's actions caused an interference with the privacy of its members and staff. As a result of the complaint, the gym instituted practices to ensure the safe disposal of information. I was satisfied that the procedures it implemented were sufficient to prevent a recurrence and discontinued my investigation of the complaint.

Organisation type

The government is the organisational grouping with the largest number of complaints made against it. This group includes agencies such as the New Zealand Police, the Department of Work and

TABLE 4: ALLEGED BREACHES 2000/01		
Alleged Breach	**Total**	**Percentage**
Information Privacy Principle (IPP) 1 - Purpose	64	5.65
IPP 2 - Source	15	1.33
IPP 3 - Collection	61	5.39
IPP 4 - Manner	25	2.21
IPP 5 - Storage	49	4.33
IPP 6 - Access	261	23.06
IPP 7 - Correction	24	2.12
IPP 8 - Accuracy	46	4.06
IPP 9 - Retention	5	0.44
IPP10 - Use	27	2.39
IPP 11 - Disclosure	258	22.79
Public Register Privacy Principle 2	2	0.18
Section 35 - Charge	2	0.18
HIPC Rule 1	15	1.33
HIPC Rule 2	3	0.27
HIPC Rule 3	11	0.97
HIPC Rule 4	7	0.62
HIPC Rule 5	24	2.12
HIPC Rule 6	86	7.60
HIPC Rule 7	24	2.12
HIPC Rule 8	18	1.59
HIPC Rule 9	1	0.09
HIPC Rule 10	7	0.62
HIPC Rule 11	77	6.80
Health Act, section 22F	12	1.06
HIPC Clause 6 - charges	3	0.27
N/A	5	0.44
Total	1132	

Income and Accident Compensation Corporation. The health sector is the next largest grouping and includes hospitals, medical centres and other affiliated health providers such as dentists, occupational therapists, counsellors and physiotherapists. The next group is "other business" which includes agencies such as retail outlets and small businesses which are not specifically identified by category. Table 5 (page 30) identifies the organisation types.

TABLE 5: ORGANISATION TYPES 2000/01		
Government	298	33.83
Other (Business)	129	14.64
Health (Other)	82	9.31
Hospital	57	6.47
Medical Centre (GP)	39	4.43
Education	32	3.63
Banking	30	3.41
Insurance	27	3.06
Local Authority	27	3.06
Telecommunications	19	2.16
Credit Reporting	17	1.93
Law Firm	16	1.81
Real Estate	14	1.60
Media	11	1.25
Debt Collection Agency	10	1.14
Voluntary Organisation	10	1.14
Private Investigator	9	1.02
Club	8	0.91
Individual	7	0.80
Landlord/Tenant	7	0.80
Direct Marketing	6	0.68
Insurance (Health)	6	0.68
Accountant	3	0.34
Industry Association	3	0.34
Religious Organisation	3	0.34
Incorporated Societies	2	0.23
Casino	1	0.11
Courts	1	0.11
Licensing Trust	1	0.11
Market Research	1	0.11
Personnel Agency	1	0.11
Political Party	1	0.11
Trade Union	1	0.11
Tribunal	1	0.11
Trust	1	0.11
Total	**881**	

Top 8 respondents

By the very nature of the information which they hold and gather, some agencies are inevitably likely to attract a large number of requests for access to information. This can then lead on to a complaint that some information has been withheld, or that the information held is not correct, or that it has been collected in a manner or for a purpose which the complainant alleges interferes with their privacy. The agencies listed in Table 6 were the most complained about in the last year. Between them they attracted 28% of all complaints.

I observed in last year's report that my dealings with the New Zealand Police were less than satisfactory and that I was frustrated that in too many cases the Police were guilty of undue delay in dealing with complaints. I am aware that there are resourcing issues, and that it is time-consuming to deal with requests for access to information. I am pleased to report that there has been some improvement in the situation in recent months, with responsibility for dealing with complaints being devolved to regional staff and a generally more helpful approach being taken.

TABLE 6: TOP 8 RESPONDENTS 2000/01

Agency	Number of Complaints
NZ Police	58
Accident Compensation Corporation	55
Department of Work and Income	40
Department of Child, Youth and Family	35
Department of Corrections	29
IRD	15
Baycorp	15
Telecom	13
Total	260

Complaints Review Tribunal

In cases which have not been amenable to settlement, I may refer complaints which have substance to the Proceedings Commissioner with a view to instituting proceedings before the Complaints Review Tribunal. If I decide not to do this, complainants are

advised of their right to take such proceedings themselves. During the year, 28 complainants have done so, and I have referred none. In respect of one complaint taken to the Tribunal the matter as it related to one defendant was struck out and the matter as it related to the other defendant was settled.

TABLE 7: COMPLAINANT REFERRALS OUTCOME 2000/01	
Carried over 1999/00	3
Struck out	13
Proceedings dismissed	5
Breach	2
Withdrawn	2
Settled	2
Resolved	1
Pending 2000/01	4
Total	**32**

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. Both investigating officers and enquiries officers are involved in presentation of workshops. I consider it to be an important adjunct to their complaints-handling role as it enables them to hear first-hand what issues are facing privacy officers in organisations. My staff also have a breadth of knowledge acquired from dealing with complaints, which they can share with workshop participants.

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 of these workshops were offered this year, ten in Auckland and ten in Wellington. I have offered the standard workshop to agencies which have 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 them 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. In addition to the health sector, I have provided tailored workshops to insurance companies, local authorities and a credit reporting 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. Of those attending, 84% said that the workshop had met their expectations and 15% of participants said their expectations had been exceeded.

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. Likewise, the success of our workshops is partly explained by the participation of Investigating Officers whose practical experience informs the educative process. There are positive advantages in hav-

ing the same body provide both compliance advice and investigative services.

One-day Privacy Forums were held in Wellington and Auckland at the beginning of the reporting period.

Printed resources

The second edition of *On the Record: A Practical Guide to Health Information Privacy* was published in July 2000.

During the year I released 15 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. The *New Zealand Herald* ran a series of articles on privacy issues in May. This series provoked a good deal of interest among the public and coincided with a sharp rise in the number of enquiries and complaints to my office.

One of the issues that received attention in the *Herald* series was the incidence of closed circuit television cameras, particularly in urban centres.

Use of closed circuit television cameras continues to be a topic which raises media interest. I commented about a new installation in Wanganui that it is important that cameras are installed only in areas where there has been an abnormal incidence of crime, rather than merely erected "to give people confidence". The latter approach is a clue to the fact that cameras do not prevent or detect all street

offences and that one of the objects of installing them is to promote a "perception of safety". Surveillance cameras may be a useful in some contexts but not in others. For example, if it is not worth monitoring the screens in "real time", one has to question whether the cameras should be left running. Another is that the evidence is that only certain types of mainly minor offences are detected. There is also evidence that some offences are detected but Police resources do not extend to doing anything about them. A full statement of the purposes and practices under which these cameras operate should be readily available to the public and signs should indicate that cameras are operating and where information about them can be obtained.

The popularly named "computer hacking" legislation was the subject of numerous media calls to my office. I have made submissions on this legislation and these are available on my website. The issues arising from the accessing of computers by authorities are some of the most contentious in this area. I spoke publicly about the range of privacy issues relating to this area.

Health information privacy is an ongoing area of public interest. Issues arising from the Gisborne cervical cancer inquiry continued this year and there was, consequently, some media attention upon the scope of the health information privacy rules. The adequacy of security safeguards for medical records was a related health privacy issue that arose several times throughout the year.

My office logged 168 media enquiries during the year.

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 is 5,500 copies. During the year four issues were released including three double issues.

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. I have recently begun releasing Private Word on my website first, enabling faster access for readers.

My Data Matching Compliance Officer continues to circulate the Information Matching Bulletin to assist those agencies involved in the process of data matching and to inform other interested parties.

ENQUIRIES

Two full time Enquiries Officers have handled 6,563 enquiries this year. The majority of these are telephone enquiries on an 0800 freephone number from individuals who require advice on their rights and entitlements under the Act, or agencies which seek clarification of their obligations. A smaller number of enquiries are in the form of written requests for information.

My enquiries staff give individuals information about the relevant provisions of the Privacy Act and what is involved in making a complaint to my office. If they have not already done so, my staff will encourage them to contact the agency directly to determine whether the matter can be resolved informally. Enquiries Officers also give compliance advice to government agencies and businesses who ask for help in complying with the Act. Feedback from public attending workshops has been that the service is well-regarded and helpful.

Enquiries received

TABLE 8: ENQUIRIES 1995-2001

	1995/96	1996/97	1997/98	1998/99	1999/00	2000/01
Telephone	*	8,440	10,606	6,356	5,232	6,104
Written	*	595	535	615	571	428
Visitor	*	*	*	*	*	31
Total	10,200	9,035	11,141	6,971	5,803	6,563
Av. per month	850	753	928	580	484	547

*** figures not available**

Last year I observed that the number of enquiries received had fallen for the second year in a row. That trend has not continued, and this year shows a significant increase over last year's figures. There was a considerable increase in enquiries during May and early June, (around 50 per day) which coincided with a series in the *New Zealand Herald* concerning privacy issues.

Many of the calls to the 0800 number are diverted to a voice mail system. Callers are invited to leave a message and my enquiries staff are generally able to return the calls the same day. This system enables my staff to spend as much time as is necessary with each enquiry and to deal with the correspondence that the enquiries generate. More enquiries were received by email this year (179

of the 428 written enquiries) and I expect this trend will continue. Our voice mail message alerts people to our website which may, in some cases, provide callers with sufficient information so that they do not require further assistance from the office.

During May and June some enquiries were not responded to. This occurred when Auckland staff moved to new premises and at the same time there was a problem in the central business district telephone system. This was as frustrating for us as it was for callers attempting to contact the office. The problem was rectified and I believe most callers ultimately were able to make contact with us.

Enquiry topics

One of the recurring themes dealt with by my enquiries staff was credit reporting and the use of credit information by agencies for purposes other than credit checking. Some issues which were identified included employees using credit reporting facilities to make unauthorised checks on business associates, acquaintances or family members, and credit agencies listing disputed debts against an individual's name. Callers have observed that every enquiry which is recorded on their credit record raises a question in the mind of a future credit provider as to their creditworthiness. As an adverse credit report can have serious repercussions for an individual, it is not surprising that the use of credit reporting information is of concern.

Some other common themes include landlord/tenant disputes, particularly where a tenant has vacated premises with rent due and the property in a state of disrepair; parents complaining about a school's decision not to release information relating about their child (for example counselling or health advice – including contraceptive information) and, on a another tack, enquiries from individuals who believe that their residential telephone has been bugged. There have even been enquiries from parents who report that their child's school refuses to check children for head lice "because of the Privacy Act"!

There is always a steady number of requests from students at various tertiary institutions for information to assist them with assignments. I am pleased to note that many of these requests come from students in the health sector. My staff direct them to our website or provide them with written materials.

Website

The website operated by my office continues to be a well-used source of information. It is regularly updated with fact sheets, case notes, reports on proposed legislation, speeches and the office newsletter *Private Word*. As many written enquiries are received by email, information from the website can be attached to responses.

My enquiries staff, along with the investigating officers, are also involved with 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 on my office website (www.privacy.org.nz/comply/comptop.html) or by contacting this office.

Two applications for authorisations were carried over from last year, with five new applications received this year. I granted two authorisations and declined five applications.

One of the applications carried over was subsequently granted. In that case, a large government institution wished to enable its trainees to receive NZQA equivalence for the on-the-job training they completed. To do this, certain personal details of the trainees and the courses they had completed were transferred to NZQA to enable the equivalence assessment to be carried out and credited. Identification numbers were to be assigned. I formed the view that the benefit to the individuals concerned from having their training NZQA-recognised would outweigh any interference that might occur to their privacy.

A further authorisation to disclose personal information was granted to a church. The fund manager of the church wished to locate individuals for whom money on deposit was held. The church had tried to contact the individuals through other means, but it had been without success. The fund manager proposed that notices

be published in the church's national and local newspapers in the hope of alerting the account holders. I took the view that the benefit to the individuals would outweigh any interference with their privacy that might occur from the limited disclosure.

One of the applications that had been carried over was declined because the organisation sought an exemption to allow practitioners records to be disclosed to supervisors for peer review. I have taken the view that an ongoing practice does not fulfil the criterion of "special circumstances" as required by section 54. An exemption is designed to enable flexibility in the privacy principles and rules where there is an unexpected or unforeseen situation or need. The exemptions that I grant cover highly specific events, and time limits and other conditions are prescribed in the exemption.

Another application arose from an employment dispute that had escalated. The employee was making various statements to a local newspaper which the employer wished to counter. The employer's lawyer sought a section 54 authorisation to allow them to disclose personal information about the employee. I declined the application for a number of reasons. I did not see that this situation presented special circumstances or raised a clear public interest. Neither was I certain that disclosing information would necessarily breach principle 11. Agencies are free to point out inaccuracies in a third party's account and to make denials. They are free to confirm information that has been put into the public arena and point out that there are other undisclosed facts. They may make general statements about applicable policies and processes. They may also set out reasons in a letter to the other party and direct enquiries to them for that statement.

A further three applications were declined primarily because the agency making the authorisation application was not the agency wishing to disclose information. I receive a number of these types of applications. It appears that some applicants are under the misapprehension that I can require a third party to disclose information. This is not the case. Sometimes there may be persuasive public interest grounds for information to be disclosed, however, there is usually no law preventing the agency from disclosing if they wish to. Certainly, the Privacy Act is not restraining the agency's actions and so it is not possible for me to grant an authorisation in those cases.

LEGISLATION

New and existing legislation has significant potential to impact on the privacy of individuals – frequently to detrimental effect, occasionally beneficial. Scrutiny of proposed laws is an especially important function of my office since, once passed, other statutes and regulations will prevail over the information privacy principles in the Privacy Act.

Of course, it is entirely open to any government and Parliament to enact legislation which treads heavily on privacy. I cannot prevent that. My role with respect to new legislation is akin to a "privacy watchdog": my bark can deter unwanted intruders or warn the occupiers of danger. However, the watchdog analogy does not fully describe my role. My staff are active in working with officials, and advising Ministers and select committees about the privacy risks or implications of proposed new legislation and in assisting to find innovative legislative solutions to achieve public objectives while preserving privacy to the maximum possible extent. To continue the canine analogy, I might be thought of as a "privacy guide dog" leading legislators around dangerous potholes.

The Cabinet Office Manual requires Ministers to signify compliance with the principles and guidelines of the Privacy Act when seeking to introduce bills into Parliament or when proposing new regulations. I am frequently consulted by officials in departments in relation to new proposals.

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

One of my explicit statutory functions is to examine any proposed legislation that may affect the privacy of individuals and to report the results to the Minister of Justice. During the year I submitted seven reports to the Minister on proposed new government legislation. In addition, I provided a report on my own proposals for legislative amendment to the Fourth Schedule of the

Privacy Act to replace the information matching rules (discussed in the information matching section of this report). I record a small selection of the legislative matters upon which I commented during the year.

Crimes Amendment Bill (No 6)

I reported last year on the introduction of the Crimes Amendment Bill to establish new computer crimes. I mentioned that a companion set of amendments establishing an offence of unauthorised access to a computer system (often called "hacking") was yet to be introduced. I added that:

> *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.*

The provisions concerning unauthorised access to computer systems were introduced in Supplementary Order Paper No 85 and did become controversial. I reported to the Minister on SOP No 85 in December 2000.

SOP No 85 was to make two principal amendments to the Crimes Act which I supported:

- broadening "crimes against personal privacy" by including the interception of non-oral private communications within the prohibition against intercepting private communications;

- creating a new offence of accessing a computer system without authorisation.

The expansion of laws against unauthorised interception of private communications to encompass communications such as faxes is an overdue and welcome reform. Similarly, the criminalising of hacking into computers is beneficial to privacy. However, the bill did not simply seek to criminalise such action. It also provided exemptions and authorisations for state intrusions of the same type. In my view, this represented a significant risk to privacy and my recommendations sought to limit state intrusion and promote appropriate control and accountability when such intrusions were warranted.

My principal recommendations included:

- Ensuring that new exemptions to the interception law cannot be made by delegated legislation;

- subjecting Internet service providers and telecommunications network operators to criminal sanctions if they retain, use or disclose private communications obtained during maintenance work (a matter I also took up in relation to the Telecommunications Bill mentioned elsewhere in this report);

- delaying exemptions from the new laws for the Government Communication Security Bureau until it is placed on a statutory footing and is subject to an interception warrant process;

- opposing the pernicious practice of police hacking into computer databases;

- calling for full and meaningful public reporting of any state practices involving intercepting non-oral communications and accessing computer systems.

My report to the Minister was duly copied to the select committee as is the usual practice and I appeared before the Law and Order Committee to give evidence in March 2001. In May the Committee posed several questions to me relating to my report which touched upon the scale of trawling or browsing through personal information. I prepared a supplementary report which I gave to the Committee on my second appearance in mid-May. One of the concerns that I had related to interception under "other laws" rather than through the use of an interception warrant. I strongly recommended that the wording be tightened up to promote transparency and accountability. At the Committee's request I also provided information about the practice in Australia, at federal and state level, of auditing compliance with interception warrants.

The Select Committee reported back on the bill after the end of the year in July. A number of the points that I raised had been addressed. I remained concerned at a provision that I believe is not tightly enough drawn allowing law enforcement access to computer systems under laws other than the Crimes Act itself. I am unaware of what the supposed authority in other laws is and therefore cannot be sure about the justification nor the conditions under which such access would be carried out. Other laws would not

provide the level of accountability contained in the Crimes Act (such as high level authorisation only for specific statutory purposes, the safeguarding and ultimate destruction of information obtained, the reporting to a judge on the specifics of particular warrants and to Parliament in more general terms). I was also concerned that an unprecedented and unheralded provision was slipped in making it a crime to disclose the existence of an interception warrant. The drafting of the provision is so wide that it makes, in my view, unwarranted intrusion into freedom of speech.

Children, Young Persons and Their Families Amendment Bill (No 3)

Several years ago I was consulted by the Department of Social Welfare about a replacement for 1986 regulations governing residential care of children and young persons (see the account in my 1996/97 annual report). The regulations affected the privacy of young people since they touched upon such matters as unannounced inspections of residences, the keeping and accessing of registers, personal visits, communication and the interception of personal correspondence. I also took an interest in the regulations dealing with internal examinations and strip searching before placement in secure care.

A primary purpose of the Department's review was to bring the old regulations into accordance with the New Zealand Bill of Rights Act 1990. Overall, the regulations improved the position for the personal privacy of young people in such residences consistent with the need for security and appropriate care.

The resultant 1996 regulations came in for scrutiny by the Regulations Review Committee in 1997. The committee made some adverse findings and recommended that the powers contained in the regulations relating to search and seizure be set out in primary legislation which should be enacted as soon as possible to replace the regulations. By 2000, officials were actively working on implementing those recommendations and consulted me on an amendment bill. While I was supportive of the basic notion that these intrusive powers should be located in primary rather than secondary legislation, I urged that consultation be undertaken among interested people outside the government on the substance of the provisions to govern residential care facilities. The opportunity to do so was not taken since the policy position was to make no substantive change to the powers.

Following the introduction of the amendment bill to Parliament I submitted a report to the Minister. While I acknowledged that it was a positive gesture to locate the powers in primary legislation, I was concerned that the legislative approach taken preserved the effect of the existing regulations while creating new powers of search and seizure in the statute. It appeared possible that this might inadvertently lead to an expansion of powers of search (as powers would be derived from both the Act and regulations). Furthermore, the resultant approach was complex, which might lead to difficulties in statutory interpretation and diminish transparency of the entire scheme of controls. I suggested that the bill require the existing regulations to expire after a certain period. This would allow their orderly replacement by a revised set of regulations developed in accordance with the new statutory framework.

While my recommendations in respect of the bill were not adopted, amending regulations were made revoking the powers relating to internal examinations in the 1996 regulations.

Electoral laws

Electoral law and practice continues to evolve. Since information about people – their entitlement to enrol, their status as an elector, and their choices as a voter – is central to electoral processes, change is bound to raise information privacy issues.

During the year my office was consulted by officials on a number of proposed electoral laws, including:

- Local Electoral Bill – issues worked through included, amongst others, the manner in which the public register provision was drafted, the workings of the suppression regime in the Domestic Violence Act 1996, and the display of candidates' details on official websites;

- Local Electoral Regulations 2000 – one of the issues concerned the means to ensure the personal safety of ratepayer nominees where those persons have special reasons to keep their details confidential;

- Education (School Trustee) Elections Regulations 2000 – in this case the Department took the innovative course of providing that while the electoral roll is to include both name and address of all voters (typically parents), only the names and not the ad-

dresses would be available for public inspection, (similarly candidates' home addresses would not be published);

- Electoral Amendment Bill (No 2) – there were two significant features of this bill for my office relating both to information matching and the secondary use of electoral information for iwi affiliation registration purposes.

Electronic voting at local body level

The Local Electoral Bill contained a radical feature which I highlighted in a letter to the Minister and in a submission to the select committee. This concerned the authorising of "any form of electronic voting" as a voting method. "Electronic" was defined to include "electrical, digital, magnetic, optical, electro-magnetic, biometric and photonic". The bill did not contain any detail about electronic voting but merely that it could be adopted only where provision for it is included in regulations.

In a letter to the Minister, I drew attention to the matter and stated:

> *This bill seeks to provide unlimited authority for the adoption of electronic voting at local body level so long as the necessary regulations are issued. To give such legislative authority thereby takes Parliament out of the picture in relation to the authorising of particular electronic voting methods. The public scrutiny of select committee hearings is also absent in regulation making. In my opinion, local democracy is too important to be used as an experimental test-bed for new technology. Public trust in the electoral process is vital to a free and open democracy. Great care should be taken in authorising the adoption of technologies for political representative elections. I question how any Government or officials could offer assurances about the use of new electronic technologies in voting processes when the proposed law is entirely open ended as to the methods that might be regulated for.*
>
> *At some stage in the future, when the issues have been fully studied, technologies have been tested thoroughly in a range of less critical circumstances, New Zealand has identified appropriate electronic voting methods in which the public has trust, it would be appropriate for primary legislation to authorise those particular methods. We are not yet at that stage.*

Noting my submission, the select committee agreed that a cautious approach should be taken to new voting methods and that they should be considered carefully. As a result they added a new requirement that regulations authorising the use of a new voting method be made only after the Minister of Local Government has consulted with representative organisations and persons likely to be substantially affected.

While the select committee's change may be welcomed, I question whether law makers should provide for "electronic voting" when they do not know precisely what is in contemplation. The bill represents a worrying approach. It suggests an enthusiasm for technology notwithstanding that at the point that the bill is passed no-one will be able to explain how electronic voting might reasonably be provided for in a way that guarantees the secrecy of the ballot, security of electoral systems, public trust and equity of access. The approach also presumes that electronic voting (and the choice between different systems) merely raises minor issues of technical detail which can safely be left to the Executive after consultation with some interested parties. It was surprising to see Parliament withdrawing from involvement in such an important constitutional matter. One of the lessons from the United States' presidential election is that election technology is a matter which should be given careful study by those responsible for authorising it. I see no place for rushing to authorise electronic voting when none of the necessary policy work has been undertaken on clear practical options nor a full public debate carried out.

Data matching as part of continuous electoral enrolment

Current electoral law provides that every three years, prior to an election, there is a re-enrolment exercise whereby all enrolled voters are required to confirm that their details remain correct. This is achieved through the dispatch of postcards to the registered addresses of electors. The postcards must be signed and returned. If a postcard is returned undelivered, or otherwise not returned, the enrolled voter is placed on a dormant roll and if they do not otherwise re-enrol they will need to cast a special vote, on election day. The Electoral Amendment Bill (No 2) will change this to a system of "continuous enrolment". While it is currently intended that similar reminder postcards be dispatched every three years there will be no obligation on individuals to return those to confirm details. Enrolled voters will be presumed to remain enrolled unless they notify a change of details themselves or unless the Electoral Enrol-

ment Centre (EEC) has some other information to suggest a change in details (for example, if the postcard is returned by New Zealand Post undelivered).

Obviously, such a change in practice runs the risk of introducing significant error into the electoral roll which would be compounded as the years go by. Accordingly, other methods are being utilised to identify voters whose details have changed or who may be eligible to enrol. A principal means by which this will be done is three new information matching programmes whereby the electoral roll will be compared with:

- motor vehicle register details;
- driver licence details;
- details held by the Department of Work and Income.

Officials have been working through the many information-related technical, operational and legal issues associated with the three new programmes with staff. The challenges in successfully operating such major data matching programmes should not be underestimated and I will report more fully next year, when at least the first of the programmes is scheduled to be operational.

Use of electoral information for iwi affiliation registers

My office has been consulted over several years on a proposal to allow the use of some electoral information for the purposes of a private body or bodies seeking to successfully establish national registers of iwi affiliations. New Zealand law makes it compulsory for eligible adults to enrol to vote and I look with concern at major proposals to allow such information to be diverted to other purposes. Such concern would normally be compounded where the information is sensitive information about ethnicity and is to be used by a private body rather than an accountable public body. A fundamental privacy principle is that personal information obtained for one purpose should not normally be used for a completely different purpose. Secondary use might also raise pragmatic concerns about deterring voters from enrolling, or declaring their Maori descent, because of concerns over the non-official use. This might especially be the case if the body receiving the information were ever found to have misused the information or otherwise acted in an inappropriate or unexpected way.

On the other hand, information held by the Registrar of Electors is one of the most comprehensive sources of information about persons of Maori descent. Given the advice of officials that there is a public interest in enabling such private registers to be established, I took the view that there was a case to allow some secondary use - notwithstanding an inroad into the privacy expectations of persons enrolling or enrolled to vote. That could be achieved, in my view, by the EEC undertaking a mail-out on behalf of any approved body running an iwi affiliation register. There would be no direct disclosure of information from the EEC to a private body. The package of materials sent out would include an explanation about what was involved and include a simple return postcard addressed to the approved body (not the EEC) for those who wished to participate. Beyond the initial mail out (and subsequent mail outs to newly enrolled voters) the Registrar of Electors would have no involvement and there would be no further use of electoral information. This would be very easily achieved in a legislative sense and would be far less complicated than what was proposed by the Government or select committee.

Unfortunately, the bill deals with the matter in a far less satisfactory way from a privacy perspective. It anticipates people who wish to participate in the iwi affiliation register returning their details to the Registrar of Electors and for the EEC to process those details and send them electronically to the approved body. This would be done on an on-going basis not simply with new registrations, but also for all change of address information as well. In other words, the EEC will be providing an address-updating service for a private body. There is also a possibility that the unique identifier assigned to all adult New Zealanders by the Registrar of Electors is now to become the identification number for the private bodies, contrary to information privacy principle 12.

In my view, the outcome is less satisfactory from a point of principle in the way it handles compulsorily acquired and sensitive information than it could have been. It unnecessarily integrates a private body's requirements and information practices into the law governing elections. A lot of the relevant policy work has also been undertaken alongside the passage of the legislation rather than preceding it.

Electricity Industry Bill

This bill was introduced to give effect to recommendations of the Ministerial inquiry into the Electricity Industry. It allowed for a code on access to information for beneficiaries of customer and consumer trusts to be established by regulations. The regulation making power was in three parts providing for:

- information access and open meeting regimes;
- a body to review contested information access and meetings decisions;
- rights of appeal or review.

While I supported information access and open meetings as appropriate accountability mechanisms, I suggested some fine tuning amendments in a report to the Minister. In particular, it was important that the access rights in information privacy principle 6 not inadvertently be diminished as a result of the overlap with any new code.

Among other observations in the report:

- I recommended that it be made clear that the new code would not limit individual rights of access provided in the Privacy Act.
- I suggested that the meetings be required to be open not only to beneficiaries (that is persons in the particular district) but also to bona fide news media. Otherwise a journalist could be excluded because he or she happened to reside elsewhere or because the newspaper was based in another district.
- The regime did not nominate a body for review of access decisions. However, the proposed Electricity Ombudsman would be suitable given that the investigative and conciliatory nature of ombudsmen processes have been proved through the Ombudsmen's office and my own;
- I opposed the attempt to oust the application of the Regulations (Disallowance) Act 1989 and noted the importance of such safeguards in relation to delegated legislation.

In an unusual move, the measure was discharged from a select committee shortly after the end of the year. The Government intended to reintroduce the measure taking into account aspects of the select committee scrutiny, including changes which would address most of the concerns I expressed.

Government Communications Security Bureau Bill

I welcomed the step taken by the Government to place the Government Communications Security Bureau (GCSB) on a statutory footing for the first time. This step accords with recommendations I have made on previous occasions and the new statutory mandate promotes transparency, certainty and legitimacy.

In my report to the Minister I acknowledged a variety of positive aspects of the bill. I had been consulted by the Department of Prime Minister and Cabinet in the preparation of the legislation and a number of the suggestions I had made were accepted. Notable features of the bill included:

- an attempt to define the objectives and functions of the Bureau and to limit GCSB's activities to those prescribed matters;
- a prohibition on unauthorised disclosure of information by GCSB;
- a full annual report with a "censored" edition tabled in Parliament and made publicly available;
- subjecting the interception of communications to a warrant process with safeguards modelled on other interception legislation;
- giving the Inspector-General of Intelligence and Security a specific function to review the appropriateness of procedures adopted by GCSB to comply with interception controls.

In my report I made a number of suggestions for change to the bill relating to both technical and substantive matters. For example, the clause providing the circumstances in which an interception required a warrant or authorisation referred at one point to the "physical connection" of an interception device to part of a network. However, there are means of interception for which a physical connection is not required, such as those utilising an induction coil to translate electromagnetic emanations into useable form.

I suggested that a further phrase be included to make it clear that a warrant is required wherever there is an interception of any private communication.

I also noted that there was a duty to minimise the impact of interception on third parties, a provision contained in other modern interception legislation which I supported. However, the bill omitted a corresponding duty in relation to authorisations for computer access. I suggested that an added duty should be to avoid damage to computer systems.

Finally, I repeated the suggestion made previously that several additional information privacy principles should be applied to GCSB. I am confident that this can be achieved without in any way hindering the operational effectiveness of the Bureau and that the principles instead represent a statutory obligation of good information practice for which there are associated accountabilities. The bill had not been reported back to Parliament by the end of the year.

Public Trust Bill

I raised several points in a report to the Minister on the way this bill (which replaces the Public Trust Office Act 1957) affects the handling of personal information.

One clause provided:

Right and powers of Minister of Finance

(1) Public Trust must furnish to the Minister of Finance, or to any officer of the Treasury authorised by the Minister of Finance, all such information as the Minister of Finance requires.

(2) Despite subsection (1), Public Trust must not, without lawful authority, disclose any information held by it in a fiduciary capacity.

There was no direct equivalent to this in the earlier Act. Subsection (2) provides an important protection for information held "in a fiduciary capacity". However, it is conceivable that Public Trust could hold sensitive personal information in other capacities. Information about employees would be an obvious example. Public Trust will also hold personal information in respect of administration of estates which may not be said to be subject to a fiduciary duty. Fiduciary duties are owed to its customers, the people for

whom it is authorised to act but not, for example, to a claimant on an estate. I was of the view that the Public Trust should not be obliged to share information gained in the administration of a particular trust or estate with a Minister of the Crown.

I suggested that the clause be made subject to secrecy requirements. One means would be to include a clause modelled upon section 18(3) of the State-Owned Enterprises Act 1986 which states:

> *The Board of a State-enterprise shall not be obliged by subsection (1) ... to supply to any Minister any information relating to an individual employee or customer of the State-enterprise, or any subsidiary of it, or any other person, if the information supplied would enable the identification of the person concerned.*

The Finance and Expenditure Committee, which considered my report, agreed with the concerns I expressed and recommended an amendment limiting the power of Ministers to require information and a further clause to require or permit Public Trust to refuse to supply information on fiduciary or privacy grounds. I set out the new clause in full since similar provisions entitling Ministers to have access to sensitive information has been included in other bills and the provision may serve as a model to show how it is possible to strike an appropriate balance. The clause provides:

> ***Refusal of request to supply information***
> *(1) A request for information under section 45 must be refused if the information:*
> *(a) is held by Public Trust in a fiduciary capacity; or*
> *(b) relates to a particular matter in which Public Trust, or any person appointed or employed by Public Trust, is required act judicially.*
> *(2) Subsection (1) applies despite any other enactment or law.*
> *(3) A request for information under section 45 may be refused if the withholding of the information is necessary to protect the privacy of a person (whether or not a natural person or a deceased person).*
> *(4) The reason for refusal in subsection (3) applies only if it is not outweighed by the requesting Minister's need to have the information in order to discharge that Minister's Ministerial duties.*

Statistics Act 1975 – Census

The five-yearly census was held in 2001. Internationally, censuses have been a "flash point" privacy issue with areas of tension ranging through the comprehensiveness or intrusiveness of the questions to be asked, the possibility of returning to certain individuals with supplementary questions depending upon their declared characteristics, administrative use of identifiable data, retention and accessing of census forms, and the coercive powers in relation to individuals who do not complete particular questions. In some European countries the sensitivities are such that a national census has been discontinued altogether.

The processes adopted in New Zealand avoid some of the features people find objectionable in some other countries. For instance, each individual completes their own form whereas in some countries, such as Australia, a single person completes a form for all members of the household. In the collection process there are also means by which privacy is preserved and there is a statutory right to refuse to answer the question about religion. There is also a degree of public confidence in Statistics New Zealand, since successive Government Statisticians have maintained the secrecy of the census and a reputation for respecting confidentiality.

One of the ongoing debates in New Zealand has been in relation to the retention of census forms after they are no longer needed for statistical analysis. The practice in some countries has been to retain the completed census forms for later public release. The Statistics Act permits the Government Statistician to take the decision to retain the census forms and for these to be placed in National Archives to be opened 100 years later. The local practice has generally been to physically destroy the census returns. This engenders public confidence in the secrecy of the census and enables the Government Statistician to give absolute assurances of confidentiality. However, since the 1960s some Government Statisticians have authorised the retention of the forms from every second census. In earlier years there was a limited degree of transparency and citizens would not necessarily have known of this decision. However, with the enactment of the Privacy Act 1993, information privacy principle 3 requires that when collecting personal information from individuals the individuals be made aware of a number of things. This would mean, in the context of the census, that individuals be told if the ultimate recipient of their completed census forms is to be National Archives with the information made publicly available at some point in the future.

If the pattern of keeping every second census had been continued, the 1996 census would have been placed in National Archives. This was the first census undertaken since the enactment of the Privacy Act. The then Government Statistician took the decision not to retain the census in National Archives. He took the view that this enabled him to give absolute assurances of confidentiality which were conducive to a successful census which was, of course, his prime responsibility. Indicating that the census returns would be retained could potentially diminish the trust residing in Statistics New Zealand and cause problems for the census through diminished cooperation or the provision of false information.

In the preparation for the 2001 census Statistics New Zealand examined the option of keeping the census on a consensual basis which offered the possibility of maintaining public trust and cooperation while allowing for the storage of forms where this was an individual's wish. Following careful study by the Department, a proposal was developed and detailed consultation with my office followed. The Department's proposal had already addressed the key privacy issues. A number of remaining matters of detail were worked through, such as whether proxy consents could be accepted (such as parents on behalf of their children) and the withdrawal of consent subsequent to the undertaking of the census.

I was satisfied with the approach ultimately taken which included:

- retention only of the individual forms, not the dwelling forms (since it would be complex to devise a suitable consent form for an entire household);

- the keeping only of individual forms where consent of the person concerned had been given, and not accepting proxy consents;

- full information as to the retention in the census form itself and the help notes;

- the right for individuals to withdraw consent for retention at any time after the census.

Individuals who wish to withdraw their consent to the retention of a census form must deal directly with Statistics New Zealand who will carry out the destruction. In the case of a dispute, a com-

plaint can be taken to the Privacy Commissioner of a breach of information privacy principle 9 alleging the continued retention of personal information for which there is no further lawful use.

Statutes Amendment Bill - Privacy Act amendments

Readers of my previous annual reports will know that I have placed a great stress on New Zealand's achieving a finding of "adequacy" by the European Union under its Data Protection Directive. The 15 EU countries have data export controls in their national laws which constrain the transfer of personal data to countries that do not offer an "adequate" level of data protection. A finding of adequacy would facilitate the free flow of personal data between Europe and New Zealand and be a significant benefit to New Zealand businesses involved in international data processing. Such a finding would also be valuable in terms of the growing number of countries outside the EU that also possess data export controls (including other European countries in the European Economic Area and those seeking to join the EU from Central Europe, plus Canada, Hong Kong and Australia).

The European Commission is undertaking a detailed examination of New Zealand law and practice in order to advise European institutions about whether a finding should be made in New Zealand's favour. Given the breadth of the study, it is not possible to predict with certainty all the issues that might be raised. However, two clear cut issues have been apparent for many years. These require an amendment to the Privacy Act if New Zealand is to have any chance at all of achieving a finding of adequacy. The amendments in question constitute the very minimum to satisfy the EU requirement. It is possible the EU may not be satisfied with those two changes, although in my opinion they should be sufficient depending upon how the EU approach develops.

The Statutes Amendment Bill introduced in December 2000 would make two amendments to the Privacy Act. The first would remove the requirement that in order to exercise a legal right of access under information privacy principle 6 a person must be a New Zealand citizen, permanent resident or in New Zealand at the time of the request. Dropping that requirement will enable European residents and others to exercise rights of access without having to travel to New Zealand. The change is not expected to be problematic for businesses or Government departments and is a change that would be justified even if New Zealand was not seeking

a finding of adequacy. It is a simple matter of fairness and good information handling practice that individuals should have such rights of access.

The second change would empower the Privacy Commissioner to issue a transfer prohibition notice in certain cases where personal information is received from another country, passes through New Zealand and is transferred onwards to a country not offering an adequate standard of data protection. The Commissioner would be empowered, but not required, to prohibit such a transfer unless measures could be taken to ensure a level of data protection consistent with international standards.

The bill had not been enacted by the end of the year.

Telecommunications Bill

Telecommunications have numerous implications for the privacy of individuals. Particularly significant are the links between communications networks and other services and technologies such as computers. The Internet, in just a few years, has changed the way we communicate and the manner in which business and government delivers services, all the while creating personal data trails and a host of privacy issues. Convergence with other technologies, such as radiocommunications, video and biometric applications, are also having profound results. The pace of technological change is unlikely to slacken any time soon.

The information privacy principles apply to the many circumstances in which telecommunications are involved in personal information handling. The Act empowers me, by code of practice, to prescribe standards that are more stringent or less stringent than the principles, or to provide how the principles should be complied with. As noted elsewhere in this report, I intend to issue a code to address telecommunications issues more precisely.

The information privacy principles are subject to the requirements of other enactments. Furthermore, there are some privacy-protective things that other enactments can do which a code of practice under the Privacy Act cannot. A simple example is to create criminal offences for intrusive behaviour. For these reasons I examined the Telecommunications Bill and submitted a report to the Minister of Justice drawing attention to two matters.

The first aspect of my report touched upon an offence provision in the existing law, which was to be re-enacted in the new Telecommunications Bill, relating to "misuse of a telephone station". Offensive telephone calls are a significant problem. Network operators have a key role in investigating complaints, counselling subscribers, denying service to offenders and, where necessary, preparing cases for prosecution. In my report, I noted that offensive calls can sometimes be characterised as an intrusion into privacy. Recipients of calls at their home perceive their private space to have been violated. Sometimes the nuisance calls also involve an element of targeted harassment, where the caller knows personal information about the person being called.

Information privacy issues also arise after offensive calls have been made. To investigate complaints the network operator will use systems data that has been generated for connection and billing purposes in order to investigate the allegations. At some point the network operator may identify the subscriber to the telephone station from which the call is made. Further investigation may reveal the identity of the caller (who may not, of course, be the subscriber). There are a number of issues about how that information is used and what is to be disclosed to the complainant – including the vexed question of whether the identity of the subscriber or caller should be revealed.

In my report I raised the matter of offensive data transmissions for consideration. When the 1987 Act was passed, businesses used facsimile machines widely, although few homes had the capacity to receive fax transmissions. Email was not in contemplation in business or home. I suggested that the offence provision be clarified if it is not clear that it applies to the transmission of offensive faxes and emails.

The second focus of my report related to the monitoring of telecommunications. The bill proposed to re-enact, without change, a clause from the 1987 Act which provided:

> *Any employee of a network operator or any person who is eligible to be declared to be a network operator may, when acting in the course of, and for the purpose of, his or her duty, intercept any telecommunications by means of a listening device or any other device for the purposes of maintaining telecommunications services.*

I recommended that the law be amended to provide that:

- any information obtained by a network operator or its employees or agents under the provision must only be used for the purposes of maintaining telecommunications services;

- such information must not be disclosed to anyone, other than the individuals concerned, except where required by law.

Those restrictions should be accompanied by an offence provision for breach.

The bill had not been passed by end of the year. However, in mid-September, the Commerce Committee reported back and accepted my recommendations in relation to the monitoring of telecommunications. A new offence provision will be applied to any person who uses or discloses information obtained under the exemption for a purpose that is not authorised by the statute. It carries a $2,000 fine ($5,000 in the case of a body corporate).

Victims' Rights Bill

In last year's annual report I noted that a Victims' Rights Bill had been introduced prior to the general election. My first report to the new Minister of Justice concerned this measure and made a number of recommendations for change. The new Government had its own policy on the subject and introduced a Supplementary Order Paper making substantial changes to the bill. I am pleased to say that many of the recommendations I made in my first report were adopted.

Having seen the new Government's proposal, I made a further report on the Victims' Rights Bill in January 2001 in which I reiterated some of the earlier recommendations that had not been adopted and offered further recommendations in relation to the new provisions.

Among other points raised in my further report:

- the withholding of victim impact statements from offenders is problematic and may not be justified;

- although the provisions of the bill were being restyled as "rights" rather than "principles" they were in most cases not enforce-

able in a legal sense and it might be appropriate to either make them fully enforceable or avoid calling them "rights";

- I made a number of drafting recommendations and also some technical recommendations concerning the interaction with the Privacy Act;

- consideration should be given to enabling victim impact statements to be delivered by a live presentation by the victim on closed circuit television or a pre-recorded videotape.

The bill had not reported back at the end of the year.

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 functions 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. Sometimes placing a complaints function with the Privacy Commissioner will be more cost effective than creating a special new procedure or complaints body, especially when complaints are expected to arise only rarely. A complaints role might be conferred upon the Commissioner if there is concern that new powers might be used in an unexpected or unreasonable way or that something might go wrong.

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. Twelve complaints alleging refusal to provide health records under

section 22F were received this year. Of those, seven were requests by parents for access to information relating to their children's medical files, and two were requests by individuals seeking health information about a deceased parent.

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.

I received one complaint under section 11B of the Social Security Act 1964. This section provides that a person may complain to the Privacy Commissioner about a breach of a code of conduct issued by the Chief Executive of the Department of Work and Income under that section. Part VIII of the Privacy Act applies to such complaints as if the code of conduct were a code of practice under the Privacy Act. The code of conduct governs demands by the Department of 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 New Zealand Customs Service. An agreement was drafted during the year with input from my office and my approval to the final agreement was given on 11 July 2001, shortly after the year ended. It is pleasing to report that this disclosure of information from the passports database, which has been taking place since 1992 without the required authority of an approved agreement, has finally been regularised.

My approval is also required under section 36 of the Passports Act in relation to agreements for the supply of information from the passports database to Australia. Further progress was made during the year towards preparing an agreement but as yet no agreement has been approved.

Consultations

The Official Information Act 1982 and the Local Government Official Information and Meetings Act 1987 require the Ombuds-

men 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 50 consultations under the two Acts were completed.

TABLE 9: CONSULTATIONS WITH THE OMBUDSMEN 1996-2001	
Year	**Number of consultations**
1996/97	87
1997/98	77
1998/99	66
1999/00	52
2000/01	50

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. In some cases I recommend making more information available than the Ombudsman's initial assessment proposes.

I have noticed that some local government bodies appear to have difficulty in responding to requests under the Local Government Official Information and Meetings Act (LGOIMA). Sometimes the difficulty arises over the interaction between LGOIMA and the Privacy Act. I have provided general advice to those bodies when it has come to my attention. In other instances, the local body seems unfamiliar with their responsibilities under LGOIMA, perhaps mistakenly believing that all requests must be dealt with in Council meetings, or considering that it is governed by the Official Information Act rather than LGOIMA. Some local bodies appear to have had difficulty in recognising a request for information and whether that request falls to be considered under the Privacy Act or LGOIMA. I have emphasised in correspondence to those local bodies that they must consider the identity of the requester and whether that person is requesting information about themselves or a third party. I have also stressed that the Privacy Act, LGOIMA and the Official Information Act work in harmony.

I encourage those local bodies to attend one of the workshops offered by my office or to contact our enquiries line, or the Ombudsmen's office, for further guidance. I am concerned that in many cases lack of training in official information leads to decisions subsequently reported as being based on the Privacy Act. Better training in Official Information Act and LGOIMA is urgently required.

I have been consulted several times in relation to the remuneration details of departmental chief executives. In fact, the release of performance pay without sufficient knowledge of the individual's job size and other relevant factors would mislead. A fair assessment of an individual's performance in a job cannot be made without knowledge of all the facts and background circumstances. Providing some information in response to a specific request can incrementally erode the privacy of the individuals involved. I am aware too, of the disincentive that disclosures of this nature can have upon prospective candidates for appointment. It is clearly Parliament's intention not to involve the responsible Minister in the remuneration of chief executives. I have taken the view that it would be anomalous, in light of this, if highly particularised performance pay details were to be released to members of the public upon request.

A considerable amount of information about chief executive remuneration is available in the State Services Commissioner's annual report.

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 10 formal meetings of the Commission during the year. In the absence of a Chief Human Rights Commissioner a greater burden fell on me at the cost and expense of the Office of the Privacy Commissioner. I chaired the meetings of the Commission and the smaller number of commissioners meant there were greater calls on my time. At year end, no compensation to this office has been forthcoming.

IV. Information Matching

INTRODUCTION

Nature of information matching and controls

Information matching usually involves the computerised comparison of two or more sets of records with the objective of seeking out records relating to the same individual in order to detect cases of interest. 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.

Information matching is perceived to have negative effects on privacy by, among other things:

- using information 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;
- requiring innocent people to prove their lack of guilt;
- 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;
- ***evaluation*** – subjecting programmes to periodic reviews and possible discontinuance.

Operational controls and safeguards

Figure 2 (page 68) illustrates something of the processes involved in authorised information matching programmes. The flowchart shown is simplified and generalised. 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 more databases involved). From each database certain records are selected e.g. only those records relating to people who have been involved in a recent transaction or activity (such as departing the country). Certain information is extracted from the records that have been selected. 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 need 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 data does indeed relate to that individual and that it is accurate and relevant.

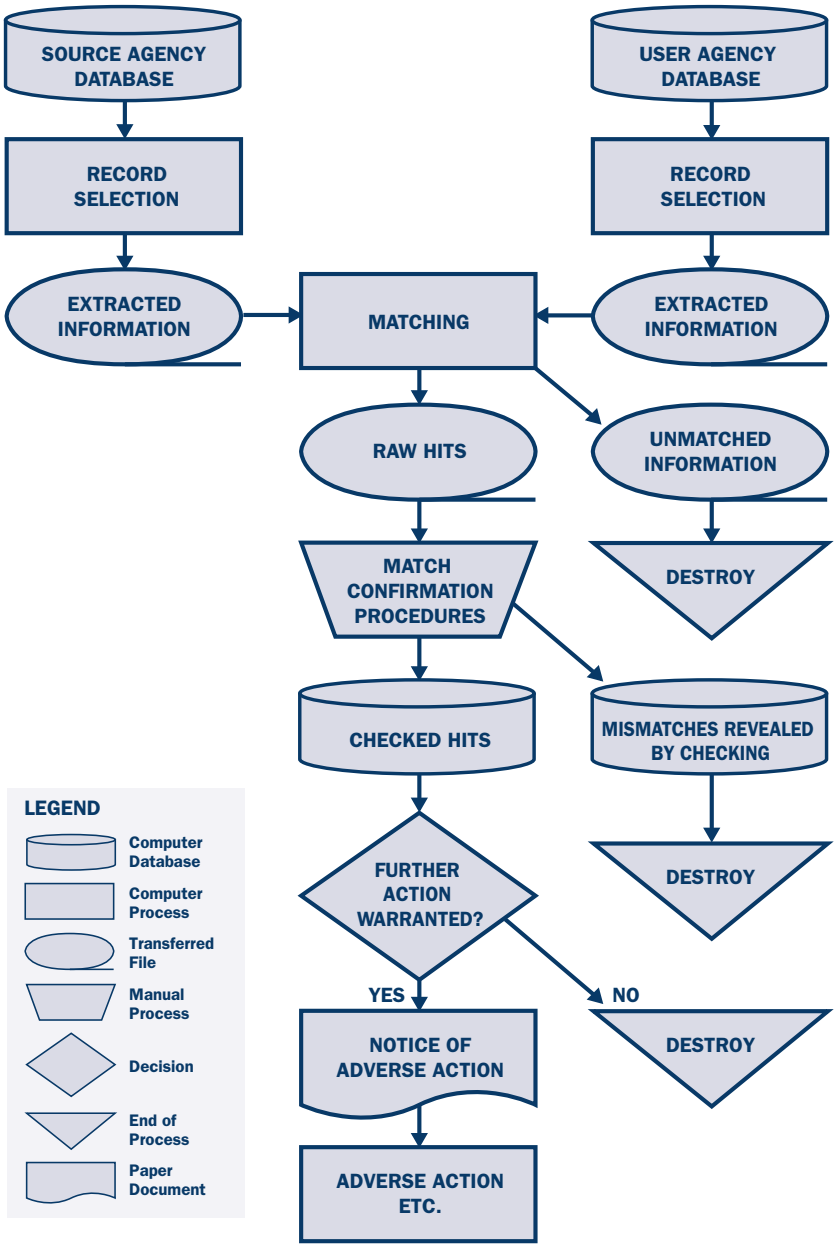
An algorithm, a process or set of rules used for problem solving, is developed and used to establish what constitutes a successful match or "hit".[3] For example, the algorithm may establish as a match – being records from the two sources likely to relate to the some person – cases where the full name, date of birth and address are all the same. It may also allow for the identification of "likely" matches even when all data do not exactly correspond, (e.g. where the surname and date of birth are the same but the first name differs) or allow for differences in the spelling of names or use a number of

1 The statutory information matching provision and the Technical Standards Report (required by information matching rule 4) both limit the information which may be used 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.

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.

Figure 2: Typical Information Matching Process



letters from the stem of a word without requiring the whole word (such as the name) to match. The process is judged likely to relate to the same person, but that cannot be said to be certain without further confirmation.

The user agency may be interested in names that occur in both lists of lists of extracted data, or those that appear in one list only. The matching results in a list of raw hits to be followed up. The information which does not show a hit of interest must not be retained.[4]

The raw hits are put through confirmation procedures.[5] Typically, that might include manually checking original records held by the user agency. The confirmation procedures may reveal some mismatches which are then destroyed.[6]

If resultant checked hits are to be used as a basis for taking action against individuals, they should be acted upon 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 be added to administrative files.[8]

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]

---

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.

9 If an agency intends 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.

New information matching initiatives

In the last year more than 30 new information matches have been mooted. Of these enabling legislation has been proposed or introduced for about 20. In large part this unusual growth in proposed matches can be ascribed to the computerisation of the birth, deaths and marriages registers.

Of the mooted matches, 21 involve the Department of Internal Affairs and in particular 19 involve the Registrar General (Births 6; Deaths 8 and Marriages 5). An observed trend in the growth of matches is the increased use of this data for purging a wide variety of other files of personal data held by government agencies e.g. Motor Vehicle Dealers Register. Automated verification of details submitted on applications is the other prominent potential use.

In addition, the Electoral Enrolment Centre has proposed three matches with the aim of identifying eligible people who appear not to be enrolled on the electoral roll and to find existing electors who have shifted or changed their details. These matches are to be with DWI (beneficiaries, superannuitants etc), Land Transport Safety Authority (licensed drivers) and the Ministry of Transport (keepers of motor vehicles). These matches involve some of government's largest people record databases.

It is not expected that all three of these matches will be implemented during 2001/02, as the systems preparation required by the source and user departments is considerable. However, with a general election next year it might be expected that at least one will have started during the 2002 calendar year.

Review of information matching rules

In January 2001, the Office sent out a discussion paper that proposed a revision of the information matching rules to all affected departments and to several beneficiary groups and others. The discussion paper gave some background to the rules, explained what it is hoped to achieve by proposed changes, and invited comment and additional suggestions for matters not covered. Together with Part X of the Privacy Act (ss.97-109), the information matching rules contained in the Fourth Schedule are the key safeguards to ensure that authorised information matching programmes are carried out fairly and successfully and in a way that protects the interests of affected individuals.

The information matching rules were first enacted into law in the Privacy Commissioner Act 1991 and have remained unchanged since. They were closely modelled upon similar guidelines in an Australian statute, the Data-Matching Program (Assistance and Tax) Act 1990. The guidelines in that Act were later replaced by guidelines issued by the Australian Privacy Commissioner and these, and another set of Australian data matching guidelines, have subsequently been revised. The proposed revised rules adopt a number of features from the latest versions of the Australian guidelines. In addition they would implement recommendations that arose out of the 1997/98 report, *Necessary and Desirable: Privacy Act 1993 Review.*

The revision of the information matching rules may contribute to the effective operation of the information matching controls by:

- expressing existing rules more clearly;
- providing new flexibility to recognise the diversity in authorised programmes;
- better integrating Part X and the information matching rules;
- using new concepts where appropriate to simplify meanings;
- enhancing protections for individuals.

The report and the suggested new Fourth Schedule to the Privacy Act 1993 is now with the Associate Minister of Justice.

Unauthorised information matching

On 30 July 1998 an article appeared in the *New Zealand Herald* reporting that the Department for Courts had incorrectly sent cards to some 4,000 people that stated that unless they paid fines within 48 hours, they would face penalties. I commissioned Auckland barrister Robert Stevens to investigate the circumstances on my behalf.

Mr Stevens' inquiries revealed that the Department for Courts had instructed EDS, who managed the operation of the motor vehicle register, on behalf of the Land Transport Safety Authority, to match a list of fines defaulters against the motor vehicle register with a view to obtaining more up to date addresses. Courts undertook not to repeat an unauthorised match.

Apart from the lack of proper preparation to ensure that matches were accurate and failing to meet the rules set out in the Privacy Act for such undertakings, it was disturbing to note that the LTSA or the Ministry of Transport were not asked to authorise the use of their data.

I adopted Mr Stevens' findings and submitted my report on this matter to the Ministers of Justice, Courts and Transport on 25 August 2000. A key recommendation was that where a public sector body entered into a data processing contract, the resulting contract should specifically prohibit the use of that body's data by another organisation without the specific approval of the body supplying the data. I was also pleased that the Controller and Auditor General drew the report to the attention of auditors while the State Services Commissioner indicated that he would include the recommendation amongst matters for action following the INCIS Ministerial Inquiry.

PROGRAMME BY PROGRAMME REPORTS

Introduction

Section 105 of the Act requires me annually to report on each authorised programme carried out during the year. This year's report covers 18 authorised programmes, of which 12 operated during the year.

Each programme bears 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/DWI Commencement/Cessations Match", IRD is given first as the source agency. DWI as user agency is given second. This programme is described as a "commencement/cessations match" which indicates something of its nature and distinguishes it from the "debtors address match" involving the same agencies.

I have classified each programme by one or more of eight primary purposes as follows:

- ***confirmation of eligibility or continuing eligibility*** for a benefit programme, or compliance with a requirement of a programme –13 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.

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
Corrections	Department of Corrections
Courts	Department for Courts
CSC	Community Services Card
Customs	New Zealand Customs Service
DWI	Department of Work and Income
EEC	Electoral Enrolment Centre
IMPIA	Information Matching Privacy Impact Assessment

IRD	Inland Revenue Department
Institution	Post-compulsory education service provider
MoE	Ministry of Education
NDMC	National Data Match Centre of DWI
NZIS	New Zealand Immigration Service
NZISS	New Zealand Income Support Service
Regulator	Accident Insurance Regulator
VOS	Verification of Study

The reports are set out in the following order:

Matches with DWI as user agency

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

Matches with other departments as user agency

H. Corrections/ACC Inmates Match
I. DWI/Courts Fines Defaulters Address Match
J. DWI/IRD Family Support Match
K. MoE/IRD Student Interest Write-off Match
L. NZIS/EEC Unqualified Electors Match

Matches which did not operate during year

M. ACC/IRD Child Tax Credit Match
N. IRD/Accident Insurance Regulator Employer Compliance Match
O. IRD/Accident Insurance Regulator Sanction Assessment Match
P. IRD/Courts Fines Defaulters Address Match
Q. NZIS/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). The programmes include the Customs match of arrivals/departures, the Inland Revenue matches with employment com-

TABLE 10: COMBINED TOTAL FIGURES FOR THE MAIN DWI NDMC PROGRAMMES 1999-2001		
	1999/00	2000/01
Overpayments established	$28,782,047	$34,772,993
Penalties applied	$7,107	$1,502
Cost of matching operation	$6,531,957	$6,110,145
Debt recovery costs[10]	$1,328,880	$1,102,517
Debts recovered	$9,856,131	$10,422,889

mencement/cessations and the family support, the Corrections match with prison admissions and DWI/Courts Fines Defaulters match.

Most 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 between "general expenses" and "overheads" has also been changed, so again the comparison with earlier years' figures is not useful. I therefore cite total figures only.

Debt categorisation

Over the last few years debt categorisation has become an increasing bone of contention between DWI and organisations representing the interests of beneficiaries, as well as this office and the Statistics New Zealand. Primarily, the issue stems from classifying debt as arising as a result of fraudulent behaviour when intent to defraud is not in fact proven, and in some cases the debt may well be the result of departmental error. The penalties imposed on individuals discovered through the 3 principal NDMC programmes are almost negligible: 9 penalties out of 37,345 overpayments.

There has been, at last, some movement in this area. The Department has now changed its practice and debt established as the result of the information matching will no longer be categorised as "fraudulent"; rather it will have the single classification of "data match debt". This certainly solves one problem which has been the implicit characterisation of the people concerned as

10 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 cost of recovering debts by deduction from current benefit payments is a cheaper process than pursuing the non-current debtors.

criminals. However, the new categorisation is not very informative and it may be helpful to consider sub-categorising the cases in a more sophisticated, yet non-pejorative, way in the future. The approach of the UK Department of Work and Pensions may be instructive here. They categorise their data match debt as resulting from either "customer error" or "official error".

Authority to request information from third parties

The NDMC received a Crown Law opinion that it should use s.11 of the Social Security Act 1964 as its authority for requesting information from third parties. Until recently the NMDC had been acting on the basis that s.12 of that Act provided the required authority to obtain information. Simply put, s.11 requires the NDMC to request the information from the individual before requesting it from a third party. The requests must comply with the departmental Code of Conduct applying to obtaining information under s.11 of the Social Security Act 1964.

While this has resulted in changes to how all information matches are processed by the NDMC, it has particularly impacted upon the processes involved in the IRD/DWI Commencement/Cessations Match. The changes have included:

- adapting call sheets;
- revising the contents of standard letters (including s.103 notices);
- development of new standard letters;
- development of manual procedures for the issue of standard letters as the automated letter production processes have had to be turned off. (However, it is planned to update the systems to incorporate changed business rules and to re-automate the production of standard letters.)

Section 103 notices

The entire range of s.103 notices relating to all the matches processed by the NDMC have been revised after consultation with my office and a representative of the Wellington People's Resource Centre. The new letters, which also incorporated the changes resulting from the shift in reliance upon s.12 to s.11 (see above), went into production at then end of this reporting year.

NDMC systems upgrade

Due to the increasing age, cost and complexity of maintaining and enhancing the current system as well as the dated technology in which it resides, the Department and the NDMC have commenced work on preparing the requirements for a replacement NDMC system.

Challenges

As a result of improvements in reporting challenges to matches, 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 the figures reported, it appears that the incidence of successful challenges to the total number of records with a debt established by the programmes is approximately as follows (last year's figures are in brackets):

Customs/DWI Arrivals & Departures Match:	1 case in 233 (180)
IRD/DWI Commencement/ Cessation Match:	1 case in 68 (40)
Corrections/ DWI Inmates Match:	1 case in 163 (850)

The drastic difference between last year's and this year's figure for the Corrections/DWI Inmates Match is in large part explained by the fact that it was necessary to play "catch up". It was discovered that Corrections had not been supplying full lists of admissions to prisons (now corrected) and so a special run was done of all inmates. This resulted in numerous challenges from people whose benefit already had a status of "cancelled" at the time that they received the notice. I will encourage DWI to continue to monitor and record such challenge figures with an eye to establishing patterns that might enhance the accuracy of the matching processes.

Matches with DWI as user agency

A. Corrections/DWI Penal Institutions Match

CORRECTIONS/DWI PENAL INSTITUTIONS 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
Online transfers	None

The Corrections/DWI Penal Institutions Match is designed to detect those persons receiving income support who are imprisoned and are ineligible for such payments. 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 that 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 11: CORRECTIONS/DWI PENAL INSTITUTIONS MATCH – 1999-2001 RESULTS		
	1999/00	2000/01
Number of runs	53	51
Number of records compared	13,640	74,331
Number of "positive" matches	5,771	24,639
Legitimate records (no adverse action taken)	3,118	16,706
Notices of adverse action issued	2,658	7,813
Debts established (number)	2,545	4,094
Overpayments established	$1,129,452	$2,238,018
Challenges	4	44
Challenges successful	3	25

The reason that the "Legitimate records" plus the "Notices of adverse action taken" do not equal "Number of positive matches" (out by 120) is due the fact that files may be received in one reporting year but action is not taken until the next.

The most obvious development in the statistical results for this programme is an increase of over 500% in the "number of records compared", with consequential increases of about 200% in the value of the debts established. These records originate in the Department of Corrections, which last year implemented a new database system ("OIMS" – Offender Integrated Management System). The Report on Data Matching activity for the period 1 July 2000 to 31 December 2000, from DWI first revealed that Corrections was under-reporting the number of admissions to prisons. Enquiries with Corrections have revealed that as a consequence of DWI advising them of a number of instances of cases of known inmates not being advised through the information matching process, Corrections undertook a review of their extract program that identified a "substantial difference" between the results achieved by the extract program and the result of a query run using alternative analysis software. Further investigation resulted in the discovery of logical flaws in the construct of the original extract program with the result that this program was completely re-written. This new program was found to produce results in line with the alternative analysis software. In consultation with DWI the extract program was replaced and one global extract was run to provide DWI with any missing data (which contributes artificially high figures for this year's "number of records compared").

This global ad hoc run was then processed using the existing National Data Match Centre application. This run alone produced a positive match (where a name matched a DWI client with a current benefit status) of 5,539 records, as well as 4,266 'exceptions' (where the status of the DWI client was 'cancelled'). The latter entries required manual checking to establish whether the benefit was current at any time during that person's incarceration.

The errors in not fully reporting all persons admitted to prison were also believed to have affected 10 of the 12 months of the 1999/2000 fiscal year with the obvious result that that year has been under processed.

Of interest is the fact that the percentage of notices of adverse action taken has dropped from last year's 19% to 11% of the number

of records compared. However, the number of "debts established" as a percentage of positive matches has dropped from last year's 44% to 17%. The main cause of the number of positive matches is the fact that the one global run (of all inmates in prison at the time) would mean that in many cases a positive match would result even though the Department had previously been made aware of the incarceration. In addition, this also explains why compared to previous years, relatively few of the s.103 notices resulted in positive action (it had already been taken when the incarceration was first reported).

I note a substantial increase in the number of challenges in the last 12 months: 44 compared with only 4 in 1999/2000. Some 25 of these challenges came as a result of the 'global' run and can, in part, be explained by the time delay between a s.103 notice being sent and when the person was actually admitted to the penal institution and the number where there was a "cancelled benefit" status when the notice was received. While the number of challenges increased, the percentage of successful challenges dropped significantly from 75% to 58% in the 1999/2000 financial year.

I have for some time been requesting that notices of adverse action, commonly referred to as "s.103 notices", be sent to both the prison address and the home address held by the DWI. Previously a notice was sent only to the prison. I requested that a notice also be sent to the home address. A notice sent solely to the prison would, in the case of a mistaken identity, fail to advise a person who is not in prison of the fact that DWI was acting on the premise that they were. I am pleased to note that this practice has been implemented with effect from 25 April 2001.

I am satisfied that this information programme is 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 of the Privacy Act and the information matching rules.

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
Online transfers	None

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

The programme operates by a transfer of passenger arrival and departure information once a week from Customs 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.

Results

The number of records received last year grew by 10% while the number of positive matches has remained constant at 0.44% of the number of records received. However, the amount of the overpayments established has increased by 38%. The number of challenges also grew in line with the growth in records received, but the proportion of the challenges which were successful decreased slightly from 76% to 73%.

TABLE 12: CUSTOMS/DWI ARRIVALS & DEPARTURES MATCH – 1998-2001 RESULTS [11]			
	1998/99	1999/00	2000/01
Number of runs	52	52	53
Number of records received from Customs	5,646,430	6,086,485	6,719,388
Number of "positive" matches	24,912	26,989	29,760
Legitimate records (no adverse action taken)	7,187	7,183	8,695
Notices of adverse action issued	18,165	19,797	20,304
Debts established (number)	13,577	12,203	16,843
Overpayments established	$7,222,958	$5,972,158	$8,263,699
Challenges	33	84	99
Challenges successful	28	64	72

I have again been advised that the initiative to produce a revised information matching agreement and Technical Standards Report have not been undertaken in the last year. The reasons for this further postponement include:

- "policy changes within DWI that are not being reflected in the output of this match"; an example is the work test policy changes that have an impact on the entitlement periods while absent from New Zealand;

- DWI's wish to "revisit some of the programme coding to improve the quality of the output". I am advised that the review of the existing coding, which has not changed since it was created in 1996, is currently under way;

- the unsatisfactory operation of the holding file is under scrutiny. This is the file that captures departure details of persons who have entitlement to income support while absent from New Zealand for a limited time. At present it is unclear whether the fault lies in a malfunction or whether the specifications of DWI's requirements are simply not being met.

11 The 1998/99 figures are as at 31 August 1999, the 1999/2000 figures are as at 17 August 2000 and the 2000/01 figures are as 30 June 2001.

On the basis that all of these issues may result in changes to the system, the Department felt it best to delay the re-write of the agreement and Technical Standards Report until these have been finalised. I will keep this under review.

This well-established information matching programme works relatively 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.

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.

TABLE 13: CUSTOMS/DWI ARRIVALS & DEPARTURES MATCH – 2000/01 – BREAKDOWN BY BENEFIT TYPE

Benefit type	Number	Total overpayments $	Median overpayment $
Unemployment	13,338	4,976,665	347
Sickness	1,695	628,116	327
Training	114	32,159	218
DPB	1,297	1,989,044	1,593
Invalid	175	192,658	1,088
Widows	117	87,063	627
Orphans	38	27,270	639
Superannuation	69	330,724	5,606
Total	12,203	$8,263,689	n/a

While there have been slight increases for all the benefit types, these can be attributed generally to the higher rates of benefits. The high median overpayment value for 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. Educational Institutions/DWI Loans & Allowances Match

EDUCATIONAL INSTITUTIONS/DWI STUDENT 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
Online transfers	None

This programme operates between the Department of Work and Income and post compulsory educational service providers (referred to as "institutions" in this report). 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:

- 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).

To receive student allowances and student loans, one of the essential criteria is enrolment in an approved post compulsory education course. There are innumerable qualifying courses, offered by over 700 separate institutions that range from the universities, polytechnics and colleges of education through to small private training establishments. Rather than requiring the student applying for a loan or allowance to produce proof of enrolment, DWI uses this information matching process to contact the institution directly for the necessary verification of study enrolment.

DWI sends to the institution the details of those applicants who claim to be enrolled with that institution for a course that qualifies for an allowance or loan. The institution matches the details of those applicants with their enrolment records and reports back to the Department. Thus the matching process is actually carried out by the institutions, with results fed back to the DWI for action.

Each institution 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 may make a manual check of their enrolment records and produce a facsimile form of feedback. Of the 720 or so institutions 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.

If the 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 DWI is because the student has not enrolled (as yet), sometimes it is because the student name does not match, and sometimes because the course the student is 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 is notified under s.103 of the Privacy Act that the application is going to be turned down, and is given opportunity to show why that should not happen.

Results

TABLE 14: EDUCATIONAL INSTITUTIONS/DWI LOANS & ALLOWANCES MATCH – VOS RESULTS 2000/01				
	Jul-Sept 2000	Oct-Dec 2000	Jan-Mar 2001	Apr-Jun 2001
Total VOS requests made	61,463	72,247	488,483	110,315
Individual applicants involved	32,088	27,397	124,400	56,065
Positive matches achieved	44,772	58,745	460,051	101,388
Confirmed eligibility	56,679	29,942	246,726	63,256
Number of institutions involved	665	547	521	490
VOS successful first time	65%	48%	36%	56%
More than 5 VOS attempts	5%	12%	24%	20%

I stated in my last report that the test of whether or not there are still some practical problems in the system will not come until the first quarter of 2001 when the first peak loading would come with students enrolling for the new academic year. There have not been any unusual problems.

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, and totals for the year for both the 1999/2000 and 2000/01 years, in tables 14 and 15.

There was, at one time, a plan to also use this matching process to confirm Results of Study (ROS). Although the framework for the ROS was put in place, the decision was taken not to implement this

TABLE 15: EDUCATIONAL INSTITUTIONS/DWI LOANS & ALLOWANCES MATCH – VOS RESULTS COMPARISON OF ANNUAL TOTALS 1999/00 & 2000/01			
	2000/01	1999/00	Variance
Total VOS requests made	732,508	480,984	251,524
Individual applicants involved	239,950	170,358	69,592
Positive matches achieved	664,956	363,213	301,743
Confirmed eligibility	396,603	224,541	172,062
Number of institutions involved	556	600	-45
VOS successful first time	51.3%	56.8%	-5.50%
More than 5 VOS attempts	15.3%	4.8%	10.5%

part of the match in the way it had been designed. I understand that there are no longer plans to implement ROS matching with the current system.

The large increase in the number of students this year is due to the fact that this is the first full year of processing loans and allowances applications.

Notification about the existence of this information matching programme is given to students when they apply for an allowance or loan.

I have not received any complaints about this programme. On the information provided to me I am satisfied that the programme has been operated in accordance with ss. 99 to 103 of the Privacy Act and with the information matching rules.

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

EMPLOYERS/DWI SECTION 11A SOCIAL SECURITY ACT MATCH	
Year authorised	1993
Match type	Detection of illegal behavior
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). 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 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 16: EMPLOYERS/DWI SECTION 11A SOCIAL SECURITY ACT MATCH 1998-2001 RESULTS (as at 22 August 2001)			
	1998/99	1999/00	2000/01
Matches approved	75	89	52
Matches completed	69	56	29
Matches not completed	6	33	23
Details of completed matches			
Total of employees checked	15,266	13,500	5,382
Cases investigated	2,278	774	720
Benefits cancelled or adjusted	1,377	543	282
Total costs	$106,574	$19,762	$16,861
Total savings	$1,682,282	$1,024,048	$368,957
Net savings per completed match	$1,575,709	$1,004,286	$352,097

Table 16 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 1998/99 have been completed as have most, but not all, of the following year's. About half of the matches approved in 2000/01 remain current and have not been completed by July 2001. Accordingly, the following table sets out results for the last two years in a broadly comparable position in the cycle.

TABLE 17: EMPLOYERS/DWI SECTION 11A SOCIAL SECURITY ACT MATCH 1999-2001 COMPARABLE INTERIM RESULTS

	1999/00 as at 19/7/00	2000/01 as at 22/8/01
Matches approved	89	52
Matches completed	56	29
Matches not completed	33	22
Total cost	$19,762	$16,860
Total savings	$1,024,048	$368,957
Net savings	$1,004,286	$352,096
Net savings per completed match	$17,934	$12,141

During the year, some work was undertaken towards reviewing the operation of this match under 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 have been completed this year and a final s.106 review report will be submitted in the coming year.

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.

E. 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 • Confimation of continuing eligibility • Detection of illegal behaviour
Unique identifiers	Tax file number
Online transfers	None

The IRD/DWI Commencement/Cessations Match is designed to detect those who are receiving a benefit and working at the same time. The programme operates by an exchange of information 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 determines 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;
- 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 18: IRD/DWI COMMENCEMENT/CESSATION MATCH - 1999-2001 RESULTS		
	1999/00	2000/01
Number of runs	7	5
Number of records compared	490,151	380,418
Number of "positive" matches	226,659	195,140
Legitimate records (no adverse action taken)	164,272	108,538
Notices of adverse action issued	38,774	30,557
Debts established (number)	16,244	16,483
Overpayments established	$21,680,438	$24,271,276
Challenges	765	707
Challenges successful	211	239

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 8 years now in more or less the same form, and appears to have reached a relatively high level of efficiency and control.

The NDMC decided not to further process the results from the tape that was created for matching on 5 April 2001 (it was processed by IRD and returned to EDS on 10 April 2001). On the advice of the NDMC that they would be unable to process the results, the data was destroyed by EDS.

The data resulting from the June run was found to be almost double that normally expected and investigations revealed that the causes were:

- software changes that were required to be made to accommodate the fact that data had been selected for the April run but did not complete the full cycle of processing (see above). As a

consequence a one-time software change was made to include all cases where a benefit had been cancelled since the creation of the tape in February;

- EDS selected 2/6th rather than 1/6th of the current clients, and

- the Area Benefit Control requests were significantly higher as they had a special investigation under way.

The result of this combination of factors is that on 28 June 2001 NDMC received a file containing 78,593 records for comparison of which 3,513 related to Area Benefit Control Teams requests. I will keep a particular watch on these and related developments.

On the basis of the information which has been supplied to me, I am satisfied that this information matching programme has been conducted in accordance with 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
Online transfers	None

The IRD/DWI Community Services Card Match 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 10,000 cases on average each time.

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. 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
Online transfers	None

The IRD/DWI Address Match 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 19: IRD/DWI DEBTOR ADDRESS MATCH - 1998-2001 RESULTS			
	1998/99	1999/00	2000/01
Number of runs	6	5	6
Debtors sent for matching (A)	342,697	293,057	348,448
Average number of debtors per run	57,116	58,611	58,075
Matched by IRD (B)	304,552	261,672	313,731
% of debtors sent (B/A)	89.9%	89.2%	90.0%
Matches found useable (C)	94,115	57,485	70,045
% of debtors sent (C/A)	27.5%	19.6%	20.1%
% of those matched by IRD (C/B)	30.9%	22%	22.3%
Letters sent out (D)	8,534	3,444	3,132
% of those matched by IRD (D/B)	2.8%	1.3%	1.0%
% of matches found useable (D/C)	9.1%	6.0%	4.5%
Letter not returned (presumed delivered) (E)	7,612	3,199	2,932
% of matches found useable (E/C)	8.1%	5.6%	4.2%
% of letters sent out (E/D)	89.2%	92.9%	93.6%

The proportion of "matches found useable" resulting in letters being sent out dropped noticeably last year from the earlier performance achieved by this matching programme, but has steadied somewhat this year. 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.

As I predicted previously, the figures for the "percentage of matches found useful" continued to decline as the IRD address data for individuals falls further out of date. Ultimately this will result in the need to review the justification for continuing this match.

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 ss. 99 to 103 of the Act and the information matching rules.

Matches with other departments as user agency

H. Corrections/ACC Inmates Match

CORRECTIONS/ACC INMATES MATCH	
Information matching provision	Accident Insurance Act 1998, s.353
Year authorised	1992
Commencement date	2000
Match type	Confirmation of continuing eligibility
Unique identifiers	None
On-line transfers	None

The purpose of the Corrections/ACC Inmates Match is to enforce the provision, now contained in s.122 of the Accident Insurance Act 1998 (to be carried forward into the replacement Act) 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.

The match started in September 2000.

Results

TABLE 20: CORRECTIONS/ACC INMATES MATCH - 2000/01 RESULTS	
Number of runs	42 (39 active)
Number of records compared	27,425
Number of "positive" matches	8,756
Legitimate records (no adverse action taken)	8,572
Debts established (number)	121
Overpayments established	$39,851
Challenges	3
Challenges successful	0

Though this match was started in September 2000 I did not receive any returns under s.104 from the ACC until an enquiry initiated by my staff revealed that the match had been activated. I subsequently received an annual return covering the period up 30 June 2001 and assurances that quarterly returns will be forthcoming in the future.

The most striking feature is that although this match is similar to that undertaken between Corrections and DWI, that match resulted in 74,331 inmate records received for comparison, whereas this match only generated 27,425 inmate records. In part this is explained by the fact that this run has not been active for a full year (42 weekly runs versus 53 by DWI). The average number of inmates per run is 638 for the ACC match and 1,457 for the DWI match. The balance of the difference is accounted for by the special single match of all prisoners run by DWI (about 25,000 records) which was not required in this case and that the count supplied by ACC did not include alias records as separate records as happens in the Corrections/DWI Inmates Match.

I note the low number of debts established, 121, with an average value of only $329 per debt, resulting in an average debt of $948 per weekly run. It may be noted that the Information Matching Agreement between Corrections and ACC provides for the ACC to reimburse the Department for both development costs and the costs incurred in providing the weekly data at $400 per week. It would surprise me if the costs of this match do not exceed the amount of debt established, let alone the amount of money actually recovered. However there may well be other reasons why this match is considered worthwhile by the ACC. I have requested that they review the value of this match.

On the information provided to me I am satisfied that the programme has been operated in accordance with ss.99 to 103 of the Privacy Act and with the information matching rules.

I. DWI/Courts Fines Defaulters Address Match

DWI/COURTS FINES DEFAULTERS ADDRESS MATCH	
Information matching provision	Social Security Act 1964
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 is an information matching programme in which the Department for Courts selects a range of its outstanding fines defaulters and sends these via electronic media to the Department of Work and Income, and which is to supply address information for any matched records in its database. The purpose of the programme is to locate those who owe fines in order to enable recovery of outstanding amounts.

Results

Three runs of this programme (Runs 25, 26 and 27) were planned in the 2000/01, year, compared with five in the previous year. However, two of these runs (Runs 25 and 26) were aborted due to corrupted data files from Courts (contaminated media is the suspected cause).

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. 1999/00 was 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.

Table 21 (page 99) sets out basic statistics for the single match run completed in 2000/01, with comparable figures for the last run of the previous year.

I note with some pleasure that the number of successful challenges as a percentage of useable matches has been reduced from

TABLE 21: DWI/COURTS FINES DEFAULTERS ADDRESS MATCH: 2000/01 RESULTS (by run date)		
Run date	1/00	25/1/01
Names sent for matching	45,161	47,581
Names matched	7,650	11,822
Useable matches	7,616	11,782
Cleared before notice	3,108	4,239
Sucessfully challenged	1,103	715
% of useable matched challenged	14%	6%
Collection instituted	1,424	3,014

14% to a more acceptable level of 6% in the more recent run. However, I caution that this reduction needs to be confirmed as a trend rather than a one-off result that the above table shows. I will continue to monitor the number of successful challenges that arise from this match.

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.

J. 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 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).

Results

TABLE 22: DWI/IRD FAMILY SUPPORT MATCH 1998-2001 RESULTS			
	1998/99 Runs 33-41	**1999/00 Runs 42-50**	**2000/01 Runs 51-59**
Cases sent by IRD to DWI for matching	878,754	935,176	1,031,512
Cases matched by DWI	6,889	8,019	10,202
Cases of adverse action taken	5,524	6,506	8,846
Costs incurred by IRD*	$460,198	$226,569	$539,381
Savings (estimated)[12]	$14,563,098	$15,055,335	$21,754,921
*See comments below relating to cost			

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

The gradual increase in the number of individuals being matched has continued in the year under report with there being 9 runs averaging 12,738 individuals (as compared to an average of 11,461 per run for the previous year). This represents an increase of 10%. The "cases matched by DWI" has grown by 27%, the cases where adverse action has been taken by 36% and the amount "savings (estimated)" by 41%. The large disparity between the costs incurred is artificially high due to last year's costs being artificially low (refer last year's annual report).

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.

K. IRD/MoE Student Loan Interest Write-Off Match

IRD/MINISTRY OF EDUCATION MATCH	
Information matching provision	Tax Administration Act 1994, s.85D
Year authorised	2000
Commencement date	2001
Match type	Confirmation of entitlement
Unique identifiers	Tax file number
On-line transfers	None

The purpose of the IRD/Ministry of Education Student Loan Interest Write-Off Match is to enable the interest that has accrued on a student loan to be written off in two circumstances:

- where a student is studying full time;
- where a student on a low income is studying part time.

The match operates by a student borrower applying to the IRD for the appropriate interest write-off by completing an application form on which they supply their IRD number, student identification (which may be numeric or alpha numeric) and educational institution code. This information is then entered into the IRD system and a file created consisting of that information for passing on to the MoE. The MoE matches the data with the returns of enrolment records supplied to it by the institutions, thus establishing the enrolment details (whether full or part time or not studying, for cases where no match was found) for a particular applicant. A record with result of the match encoded is then returned to IRD. It should be noted that where a student is enrolled at more than one provider the process of sending the application details (multiple student identifiers and institution codes) is based on hard copy and the matching process is by manual enquiry of the MoE enrolment database.

IRD processes the results of the match by either updating its records to indicate whether the borrower is a part time or full time student or, in cases where the MoE provides a not-studying return (no match or course of study does not qualify), a letter is sent to the applicant (s.103 notice).

The s.103 notice advises that the MoE was not able to confirm study status under the student number and provider code provided by the student. The student number and provider code as sent to the MoE is shown in the notice.

In the event that the number is incorrect or the borrower is studying at more than one provider (and consequently there are additional numbers or codes to provide) further action is required:

(a) for the borrower to provide this additional information via 0800 numbers; or

(b) for purely numerical responses the borrower can also advise IRD using the write-off form on the IRD website.

In the event that the borrower has no corrections to make or additional numbers to provide then the applicant is told "you'll need to ask the Ministry of Education to check their records with your tertiary provider". A study confirmation form 'IR 887' is included with the s.103 notice to enable this enquiry to be made. The enquiry can be initiated via the Internet.

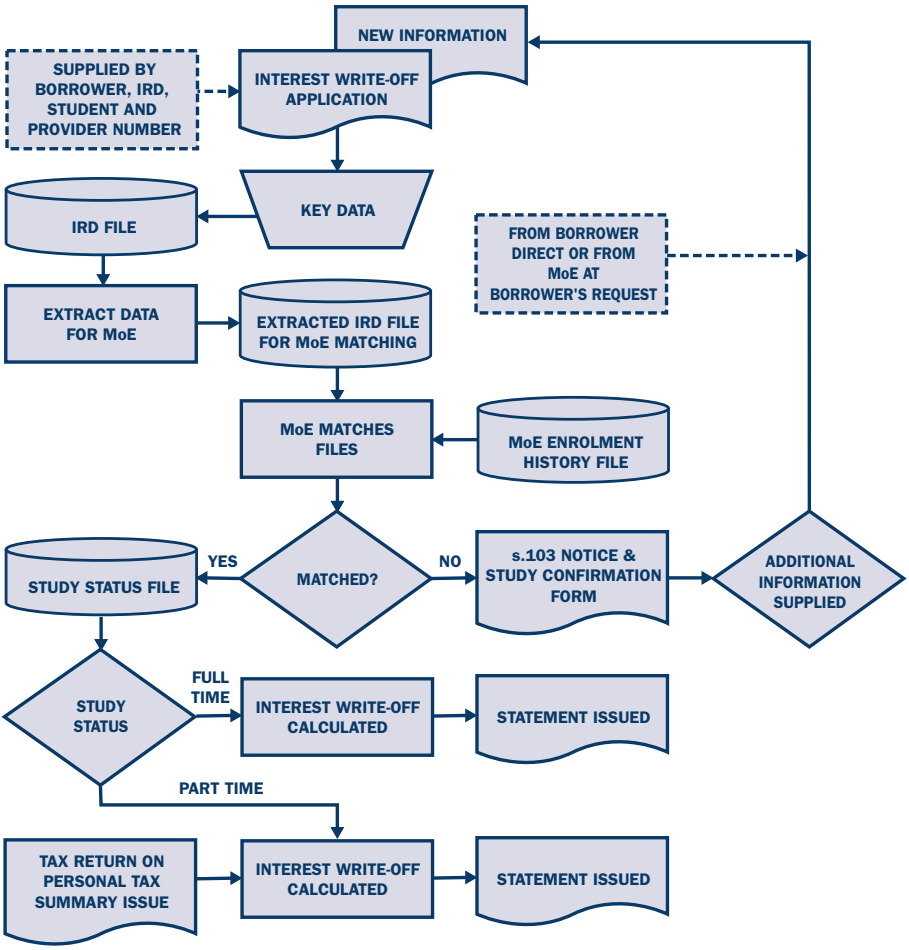
Borrowers are advised that a reply from the Ministry will be forthcoming within "four weeks" of receipt of the study confirmation form and if nothing has been heard after that time that they can contact the Ministry on an 0800 number.

Finally, if there is no record of the borrower studying, then the IRD undertakes to write to the borrower accordingly. However, if the check by the MoE in response to a borrower-initiated "confirmation of study" confirms that they were studying full time, an up-to-date loan statement is sent showing the interest write-off. If the response is studying part time, the interest write-off calculation and issue of the statement is delayed until a tax return is received or a Personal Tax Summary is issued confirming their income level.

For full time student borrowers whose study status is confirmed by the match, the interest write-off is calculated and an updated loan account statement issued. For part-time students the interest write-off is calculated when their income level has been confirmed either by the filing of a tax return or the issue of a personal tax summary after which an updated statement is issued.

Figure 3 is a diagram of this process.

Figure 3: IRD/MoE Student Loan Interest Write-off Match Process Diagram (as advised by IRD)



Discussions are continuing with the IRD concerning the procedures that are followed when a match fails. The presumption of IRD, stated in its s.103 notice, is that the match has failed as the result of the borrower supplying incorrect information (either student number or provider code) and does not take into account the possibility of errors made being made by either IRD (e.g. incorrectly keying in the data), MoE or the educational institution. All remedial action must be undertaken by the applicant.

TABLE 23: IRD/MoE STUDENT LOAN INTEREST WRITE-OFF MATCH – 2001 RESULTS

	April 2001	May 2001[13]	June 2001	Totals
Total number of IRD records sent	79,306	6,979	2,902	89,187
Number of records matched	73,571	5,900	2,088	81,559
Number of unmatched records	5,577	897	764	7,238
Total number confirmed full time students	54,585	2,366	1,444	58,395
Total number confirmed part time students	18,986	3,534	644	23,164
Failed matches[14]	158	182	50	390

Results

The interest written off as the result of this match, between 1 April and 31 May was $52,336,123.

Future matches

It should be noted that this particular match will run for the 2001 academic year only, as it is intended that next year's equivalent match will be initiated by data supplied by the Ministry of Education and matched by IRD (with data travelling in the oppo-

13 These are the combined figures of automated and manual matches (those in respect of students studying at more than one provider.

14 "Failed matches" are, for automated matched, where the data on the IRD file has altered between the time it was extracted and when the response from the Ministry is processed so the result cannot be updated, and for manual matches it is those where the IRD tax file number has been incorrectly provided by the Ministry. Remedial action is instigated within 2 days.

site direction to this year's match).

From next year, the IRD is contemplating running the programme in such a manner that it will be unable to issue s.103 notices for unsuccessful matches (as the information to be provided by the Ministry does not include a current address for the student to enable the addressing of a notice). There is no legislative authority to ignore the statutory requirement of s.103 and the departments concerned need to ensure that their arrangements can fully comply (e.g. by continuing the approach taken this year).

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

L. 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 NZIS/EEC 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 New Zealand 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.

The programme did not operate in this financial year, (although it ran both in the 2000 and 2001 calendar years outside the reporting periods).

Matches not yet brought into operation

M. 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 seeks to facilitate the exchange of information between ACC and IRD for the purpose of verifying entitlement to the Child 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. The section further empowers ACC 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 are discussions under way planning for implementation over the next 12 months.

N. 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 eligibilty • Detection of illegal behaviour
Unique identifiers	Tax file number
On-line transfers	None

The purpose of this programme is to detect individuals wrongly 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 has not become operational. I am now advised that December 2001 is the current implementation target.

O. IRD/Accident Insurance Regulator Employer Compliance Match

IRD/ACCIDENT INSURANCE REGULATOR 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 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 1998/99 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.

This employer compliance information matching programme has not been operated in the last 12 months and is not expected to be reactivated in light of the legislation returning the levy collection function to the ACC and the winding-up of @Work. However, the provisions authorising this, and the Sanction Assessment Match, have not been repealed and they each remain information matching provisions.

P. IRD/Accident Insurance Regulator Sanction Assessment Match

IRD/ACCIDENT INSURANCE REGULATOR SANCTION ASSESSMENT MATCH	
Information matching provision	Accident Insurance Act 1988, s.370
Year authorised	1998
Commencement date	2000
Match type	Updating of data
Unique identifiers	Tax file numbers
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 thence a penalty sum payable by the employer.

The operation of this programme in the first half of 2000 was described in last year's report.

This penalty-assessment information matching programme has not been used since April 2000 and is not expected to be reactivated in light of the legislation returning the levy collection function to ACC.

Q. IRD/Courts Fines Defaulters Address Match

IRD/COURTS FINE 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

Pursuant to the IRD/Courts Fines Defaulters Address Match, the Department for Courts is to be supplied by IRD with address and telephone number 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.

In light of the fact (mentioned above in the commentary on the IRD/DWI Debtor Address Match) that IRD address details for employees will become increasingly outdated as a result of changes in the requirement to furnish income tax returns, the value of the proposed match may warrant reconsideration.

R. 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 anticipates the Department of Labour, which in this context will mean the New Zealand 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 ten years ago it has never operated. DWI advised that the match is not likely to be progressed in the near future.

V. Financial and Performance Statements for the Year Ended 30 June 2001

CONTENTS

Statement of Responsibility

In the financial year ended 30 June 2001, the Privacy Commissioner accepts responsibility for the preparation of the financial statements and the judgements used therein.

The Privacy Commissioner accepts responsibility for establishing and maintaining a system of internal control designed to provide reasonable assurance as to the integrity and reliability of financial reporting.

In the opinion of the Privacy Commissioner, the financial statements for the financial year reflect fairly the financial position and operations of the Office of the Privacy Commissioner.

B H Slane
PRIVACY COMMISSIONER

Privacy Commissioner Statement of Accounting Policies for the Year Ended 30 June 2001

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 2001

1999/2000 Actual $		2000/2001 Actual $	2000/2001 Budget $
	INCOME		
1,864,889	Operating Grant	1,953,778	1,953,776
28,754	Foreign Affairs Grant	–	–
150,437	Other Income	157,141	132,350
21,248	Interest	24,940	19,000
35,735	Fixed Asset Adjustment	240	-
2,101,063	**TOTAL INCOME**	**2,136,099**	**2,105,126**
	EXPENSES		
74,229	Marketing/Newsletter	95,381	83,500
6,500	Audit Fees	8,000	8,500
66,758	Depreciation	72,138	70,096
231,680	Rental Expense	252,441	215,083
454,218	Operating expenses	551,986	475,733
1,155,466	Staff Expenses	1,335,560	1,253,974
1,988,851	**TOTAL EXPENSES**	**2,315,506**	**2,106,886**
112,212	**NET OPERATING (DEFICIT)/SURPLUS**	**(179,407)**	**(1,760)**

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

STATEMENT OF MOVEMENT IN EQUITY FOR THE YEAR ENDED 30 JUNE 2001

1999/2000 Actual $		2000/2001 Actual $	2000/2001 Budget $
191,638	Public Equity at 1 July 2000	303,850	317,850
112,212	Excess of Income over Expenses for the year	(179,407)	(1,760)
112,212	**Total recognised Revenue and Expenses for the year**	**(179,407)**	**(1,760)**
303,850	**Public Equity at 30 June 2001**	**124,443**	**316,090**

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

STATEMENT OF FINANCIAL POSITION AS AT 30 JUNE 2001

1999/2000 Actual $		Note	2000/2001 Actual $	2000/2001 Budget $
303,850	Surplus from operations		124,443	316,090
303,850	**PUBLIC EQUITY**		**124,443**	**316,090**
	Represented by:			
	ASSETS			
	Current Assets			
450	Cash on Hand		450	450
216,136	Short-term investments		84,145	278,490
7,300	Debtors		14,713	8,000
23,480	Inventory		36,001	23,480
10,238	Prepayments		10,323	10,200
257,604	***Total Current Assets***		**145,632**	**320,620**
193,164	***Fixed Assets***	**2**	**140,968**	**183,068**
450,768	**Total Assets**		**286,600**	**503,688**
	LIABILITIES			
	Current Liabilities			
146,918	Sundry Creditors	1	162,157	187,598
146,918	***Total Current Liabilities***		**162,157**	**187,598**
303,850	**NET ASSETS**		**124,443**	**316,090**

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

STATEMENT OF CASH FLOWS FOR THE YEAR ENDED 30 JUNE 2001

1999/2000 Actual $		2000/2001 Actual $	2000/2001 Budget $
	CASH FLOWS FROM OPERATING ACTIVITIES:		
	Cash was provided from:		
1,864,889	Government Grant	1,953,778	1,953,776
195,733	Other Income	149,728	131,650
21,248	Interest	24,940	19,000
2,081,870		**2,128,446**	**2,104,426**
	Cash was applied to:		
740,707	Payments to Suppliers	900,168	786,925
1,147,030	Payments to Employees	1,329,588	1,254,416
38,926	Payments of GST	10,515	(59,269)
1,926,663		**2,240,271**	**1,982,072**
155,207	**Net Cash Flows applied to operating activities**	**(111,825)**	**122,354**
	CASH FLOWS FROM INVESTING ACTIVITIES		
	Cash was applied to:		
192,708	Purchase of Fixed Assets	20,166	60,000
(192,708)	**Net Cash Flows applied to Investing Activities**	**(20,166)**	**(60,000)**
(37,501)	Net decrease in cash held	(131,991)	62,354
254,087	Plus opening cash	216,586	216,586
216,586	**Closing Cash Balance**	**84,595**	**278,940**
450	Cash on Hand	450	450
27,098	Countrywide Bank	17,711	78,490
189,038	Countrywide Bank - Deposit	66,434	200,000
216,586	**Closing Cash Balance**	**84,595**	**278,940**

The accompanying accounting policies and notes 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 2001

1999/2000 Actual $		2000/2001 Actual $	2000/2001 Budget $
112,212	Net surplus/ (deficit) from operations	(179,407)	(1,760)
	Add (less) non-cash Item:		
66,758	Depreciation	72,138	70,096
(35,735)	Fixed Asset Adjustment	224	–
31,023	**Total non-cash items**	**72,362**	**70,096**
	Add (less) movements in working capital items:		
(8,531)	Increase (Decrease) in Creditors	15,239	54,680
(2,237)	(Increase) Decrease in Prepayments	(85)	38
6,198	(Increase) Decrease in Inventory	(12,521)	–
16,542	(Increase) Decrease in Debtors	(7,413)	(700)
11,972		**(4,780)**	**54,018**
155,207	**Net Cash Flows from Operations**	**(111,825)**	**122,354**

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

STATEMENT OF COMMITMENTS AS AT 30 JUNE 2001

	2001 $	2000 $
Capital Commitments approved and contracted	**–**	**–**
Non-cancellable operating lease commitments, payable:		
Less than one year	199,110	206,500
one – two years	157,443	62,500
two - five years	409,830	20,834
Greater than five years	136,610	–
	902,993	**289,834**

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

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

STATEMENT OF CONTINGENT LIABILITIES AS AT 30 JUNE 2001

There are no contingent liabilities as at 30 June 2001. There was one contingent liability, for litigation costs of $10,000 as at 30 June 2000.

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

NOTES TO THE FINANCIAL STATEMENTS FOR THE YEAR ENDED 30 JUNE 2001

Note 1: SUNDRY CREDITORS

1999/2000 $		2000/2001 $
52,719	Accruals - Wages and Holiday pay	59,414
23,199	Trade Creditors	70,614
51,671	Accruals	23,315
19,329	GST	8,814
146,918	**TOTAL SUNDRY CREDITORS**	**162,157**

Note 2: FIXED ASSETS

	1999/2000			2000/2001		
	Cost/$	Accum Depn/$	Closing Bk Val/$	Cost/$	Accum Depn/$	Closing Bk Val/$
Office Equipment	160,394	126,837	33,557	163,286	141,212	22,074
Furniture & Fittings	52,645	49,975	2,670	35,270	34,310	960
Computer Equipment	320,588	163,651	156,937	333,005	215,071	117,934
	533,627	**340,463**	**193,164**	**531,561**	**390,593**	**140,968**

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 2001 is: -

1999/2000 $		2000/2001 $
216,136	Bank Balances	84,145
7,300	Debtors	14,713
223,436		**98,858**

Note 4: EMPLOYEES' REMUNERATION

The Commissioner has been requested to implement a Cabinet decison seeking Crown entities to disclose certain remuneration information in their annual reports. In essence, the information to be reported is the number of staff and Commissioners receiving total remuneration of $100,000 or more.

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

Remuneration of Commissioners and Staff over $100,000 pa.

Total Remuneration pa	Number
$180,000 - $200,000	1
$160,000 - $180,000	1
$140,000 - $160,000	1
$120,000 - $140,000	0
$100,000 - $120,000	2

The Commissioner's remuneration and benefits is $174,275 (in 2000 $169,336).

STATEMENT OF OUTPUTS, STATEMENT OF PERFORMANCE FOR THE YEAR ENDED 30 JUNE 2001

Output - operations of the Privacy Commissioner

	2001 $	2000 $
Total cost of producing output	**$2,315,506**	**$1,988,851**

OUTPUT 1 – CODES OF PRACTICE

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

Quantity

1. Release public issues paper/ resource document on telecommunications privacy issues in July 2000 as a precursor to notification of draft Telecommunications Information Privacy Code for public consultation.

2. Release draft Credit Information Privacy Code of practice for public consultation and subsequent issue.

3. Consider any other application for a code or any which the Commissioner should initiate (including CCTV surveillance in public places).

Achievement

1. *Privacy on the Line: A resource document in relation to Privacy in Telecommunications* was released in July 2000. A draft code was released in June 2001 for preliminary public consultation.

2. Draft code released in June 2001 for preliminary public consultation.

3.
- An application was received from the Ministry of Justice for an amendment to the Justice Sector Unique Identifier Code 1998. Discussions are continuing.

- A new code was sought by Ministry of Education and, following public notification and consultation, the Post-Compulsory Education Unique Identifier Code was issued in August 2001.

Quality	Achievement
All proposals for Codes of Practice will be the subject of public consultation and consultation with stakeholders.	Achieved. Preliminary public consultation drafts of the Credit Information Privacy Code and of the Telecommunications Information Privacy Code were issued. The Ministry of Education proposed a new code for the post-compulsory sector. Public notification of the proposal was given and a consultation process followed up to the end of the reporting period.
All issued codes are referred to the Regulations Review Committee of the House of Representatives.	Achieved.

Timeliness	Achievement
Draft Telecommunications Information Privacy Code of Practice released for public consultation not later than December 2000.	Not achieved. A draft code was released in June 2001 for preliminary public consultation.
Draft Credit Information Privacy Code of Practice released for public consultation not later than October 2000 with a view to issue by June 2001.	Not achieved. A draft code was released in June 2001 for preliminary public consultation.

OUTPUT 2 – LEGISLATION

To peruse and report upon proposed legislation.

Quantity	Achievement
1. Review of the Privacy Act	1.
● To progress vigorously changes to Act needed to get 'whitelist' status from European Union and other changes to give competitive edge to New Zealand electronic commerce, export and service industries.	The Statutes Amendment Bill implementing necessary changes to the Privacy Act to achieve EU approval was promoted strongly by the Office.
● To progress other changes to the Act particularly to progress recommendations for efficiency objectives and lower compliance costs and to make changes urgently to public register provisions to provide greater personal security for individuals in their homes.	● No progress was achieved.
● To support Minister of Justice work on the review of the Act.	● A substantial report concerning the Act was prepared for the Minister.
2. To complete reports to Minister on new bills, to meet the requirements of the Parliamentary process.	2. Seven reports were completed and provided to the Minister.
3. To continue to provide first class practical advice to departments on privacy issues and fair information practices arising in proposed legislation and in administrative proposals. Where requests are made for substantial and urgent advice to seek departmental contributions to cost of employment of contractors.	3. Advice was provided to departments through correspondence, consultations and general enquiries. Departmental contributions to offset the cost of providing this advice have not been requested this year, except for travel costs on occasions.

Quality	Achievement
All advice provided by the Commissioner or by suitably qualified staff.	Achieved.
To act on feedback obtained from recipients of advice.	Advice tailored to particular circumstances.

Timeliness	Achievement
To ensure that all advice is given to enable the introduction of the amendment bill by 30 December 2000.	Achieved. Advice tendered to Ministry and later the Select Committee.
Within the resources of the office, to give advice within a time span that will enable it to be useful to the recipient.	Submissions, reports or comments were made within the target time on all legislative proposals on which the office could usefully comment.

OUTPUT 3 – INFORMATION MATCHING

To monitor and report on information matching, and
To review statutory authorities for information matching

Quantity	Achievement
New information matching programmes: To consider and prepare reports and assist departments in relation to two new information matching programmes.	The Office considered information matching programme impact assessments during the reporting period.
To endeavour to monitor and report on 12 authorised information matching programmes. Note: The Commissioner may not be able to comply with statutory duties in respect of reporting on programmes for which no baseline funding has been approved.	Achieved.
To publish two information matching bulletins.	Achieved.
To complete section 106 reviews in respect of no less than 3 authorised information matching programmes.	The reviews were not completed in the reporting period. One batch was well advanced and one batch newly commenced.
To continue to seek funding from departments benefiting from information matching programmes so that the monitoring is regarded as an auditing function paid for by the department conducting the match. As soon as funding is secured to employ a full time staff member to be based in Wellington. Performance standards will not be attained in this area until employee can be obtained.	A full-time staff member has been employed. No funding has been agreed to.

Quality	Achievement
All parties to authorised information matching programmes will receive an information matching bulletin at least twice per year.	Two bulletins were published and distributed to relevant parties.
Reports to be published will be submitted to relevant departments for comment before publication.	Achieved.

Timeliness	Achievement
Section 106 reviews will be undertaken on no less than 3 matches before 30 June 2001.	Not achieved within specified time.
A report on all information matching programmes will be included in the Annual Report for the period ending 30 June 2001.	Achieved. The report of authorised information matching programmes is contained in the annual report.

OUTPUT 4 – COMPLAINTS RESOLUTION AND COMPLIANCE

To handle complaints of interference with privacy, and

To consult with the Ombudsman under the Official Information Act and the Local Government Official Information and Meetings Act.

Complaints resolution and compliance

Quantity	Projected	Achieved
Number of complaints received	850	881
Commissioner initiated investigations and s.13 inquiries	8	8
Total current matters requiring investigation	858	1041
Number of current complaints and backlog processed to completion or settled or discontinued in accordance with previous practice	915	805
Number of complainants advised to proceed direct to Complaints Review Tribunal	5	38
Number of s.13 inquiries completed	8	2

Quality	Achievement
● The investigation of complaints will meet or exceed the internal standards as stated in the document, "Qualitative and Quantitative Standards for the Investigation of complaints".	● Achieved. All complaints were handled to the specified internal standards.
● All complaints received by the Office are handled by suitably qualified staff working under supervision and each complaint is subject to full review by the Privacy Commissioner prior to its completion.	● Achieved.

Timeliness

- Correspondence from parties to be answered effectively within 10 working days or, alternatively, if the response is substantive, i.e. a provisional opinion, within 10 working days each party will be advised that a report is being prepared for the Commissioner.

Achievement

- Achieved. In some cases time limits would have been exceeded due to limitations of resources.

Consultation with Ombudsmen

Quantity	Projected	Achieved
Provide advice under Official Information Act and Local Government Official Information and Meetings Act to Ombudsmen on references by them.	65 – 75	50

Quality

- The advice is provided by the Commissioner.
- The advice provided is perused by the Ombudsmen and can be challenged by them.

Achievement

- Achieved.
- On occasion, further correspondence on a specific matter will follow the initial consultation.

Timeliness

- To provide advice within 20 working days or within 20 days advise the Ombudsmen that a particular matter will require longer consideration.

Achievement

- Achieved. Staff between the offices liaise over matters requiring further consideration. In some cases time limits would have been exceeded due to limitations of resources.

OUTPUT 5 – EDUCATION

To increase awareness and understanding of the Privacy Act.

Quantity	Projected	Achieved
Education workshops and conference presentations	20	56
Publication of case notes	15	15
Publication of newsletters	6 single issues	4 (including 3 double issues)
Presentation at conferences/seminars	10	13
Maintenance of website	Monthly	Fortnightly
To continue privacy helpline on reduced basis	Attended	Attended
Anticipated number of enquiries	6,000	6,563

Quality	Achievement
All enquiries received by the Office are handled by suitably qualified staff working under supervision.	Achieved.
All workshops undertaken by the Office incorporate a participants' evaluation form. In 90% of cases the evaluation will show that the expectations of participants were met or exceeded.	Exceeded. Evaluation forms showed that the workshops met expectations for 84% of participants; exceeded expectations for 15%; and did not meet for 1%.)
All enquiries are processed to meet or exceed the internal standards.	Achieved.

Timeliness	Achievement
A timetable for workshops to be conducted by the Office will be kept current and distributed to potential participants at least four times per year.	Achieved. Timetable was regularly sent to individuals on the mailing lists and is available on website.
Education workshops will be available in Wellington and Auckland each calendar month. Other regions as demand requires.	Achieved.
Telephone enquiries will be responded to at the time of the call or within 3 working days thereafter.	Achieved. Shifting offices during the year led to a short period during which enquiries were not responded to in specified time.
Written, facsimile and email enquiries will be responded to within 10 working days.	Achieved.

Additional Outputs

- 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.
- Informal enquiries, in-person visits and requests for materials were handled but were not formally logged as enquiries.
- Fact sheets prepared by senior staff covering the Privacy Act and the Health Information Privacy Code were supplied on request.
- The average print run for *Private Word* is 5,500. The mailing list continues to grow.
- The website was maintained at least fortnightly.
- Fifty-six seminars and workshops were presented during the year by qualified and experienced staff of the Office.
- The Privacy Commissioner recorded 168 requests by the media throughout the year. Other requests are received and not formally logged.
- All media statements and the majority of public speeches were made by the Privacy Commissioner personally.

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 2001

We have audited the financial statements on pages 116 to 137. The financial statements provide information about the past financial and service performance of the Privacy Commissioner and its financial position as at 30 June 2001. 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 2001, the results of its operations and cash flows and the service performance achievements for the year ended 30 June 2001.

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 the 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 Account-

ants 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 137:

- comply with generally accepted accounting practice; and
- fairly reflect:
- the financial position as at 30 June 2001;
- 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 26 October 2001 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