

# Privacy Commissioner

Annual Report 2010





Privacy Commissioner  
Te Mana Matapono Matatapu

Published by the Office of the Privacy  
Commissioner  
PO Box 10094  
Wellington  
109-111 Featherston Street  
Wellington 6143

© 2010 The Privacy Commissioner

ISSN 1179-9838 (Print)  
ISSN 1179-9846 (Online)

# ANNUAL REPORT OF THE PRIVACY COMMISSIONER

For the year ended 30 June 2010

Presented to the House of Representatives

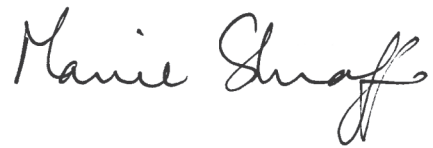
Pursuant to section 24 of the Privacy Act 1993



November 2010

**THE MINISTER OF JUSTICE**

I tender my report as Privacy Commissioner  
for the year ended 30 June 2010.

A handwritten signature in black ink, reading "Marie Shroff". The signature is written in a cursive style with a large, stylized initial 'M' and a long, sweeping tail on the 'f'.

Marie Shroff  
Privacy Commissioner

# CONTENTS

1: KEY POINTS .....	9
2: INTRODUCTION .....	13
3: OFFICE AND FUNCTIONS OF THE PRIVACY COMMISSIONER .....	19
Independence and competing interests .....	19
Complaints .....	19
Education and publicity .....	19
Legislation and policy .....	20
Information matching programmes .....	20
Codes of practice .....	20
Functions under other enactments .....	21
Reporting .....	21
Equal employment opportunities .....	21
Staff .....	23
4. REPORT ON ACTIVITIES .....	25
International activities .....	25
Highlights .....	26
Information services .....	27
Enquiries .....	27
Training and education .....	28
Privacy Awareness Week .....	28
Youth advisory group .....	28
Other outreach .....	29
Media .....	30
Complaints and access reviews .....	30
Complaints received .....	31
Complaints closed .....	32
Age of complaints .....	34
Complaint outcomes .....	35
Agency types .....	36
Top respondent agencies .....	36
Settled complaints .....	38
Personal contact and settlement .....	38
Satisfaction survey .....	38
External audit .....	39
Litigation.....	39
Human Rights Review Tribunal .....	39
Judicial review .....	41
Commissioner initiated inquiries .....	41
Google's collection of information from WIFI networks .....	41

# CONTENTS

Section 54 authorisations .....	42
Policy .....	43
Health policy .....	44
Technology policy .....	44
Law Commission's review of privacy .....	45
Information matching .....	45
Legislation .....	45
Codes of practice .....	46
Consultations with the Ombudsmen .....	46
5. INFORMATION MATCHING .....	49
Information matching and privacy – an introduction .....	49
Glossary .....	51
The year in information matching .....	52
Highlighted errors .....	53
Outreach .....	54
Changes in authorised and operating programmes .....	54
Online transfer approvals .....	55
Programme reports .....	57
1. Corrections/ACC Prisoners Programme .....	57
2. IR/ACC Levies and Compensation Programme .....	58
3. Citizenship/BDM Citizenship by Birth Processing Programme .....	58
4. BDM/DIA(C) Citizenship Application Processing Programme .....	59
5. BDM/DIA(P) Passport Eligibility Programme .....	60
6. Citizenship/DIA(P) Passport Eligibility Programme .....	61
7. NZTA/EEC Unenrolled Voters Programme .....	62
8. MoT/EEC Unenrolled Voters Programme .....	62
9. MSD/EEC Unenrolled Voters Programme .....	63
10. Citizenship/EEC Unenrolled Voters Programme .....	64
11. INZ/EEC Unqualified Voters Programme .....	65
12. BDM(Deaths)/GSF Eligibility Programme .....	65
13. BDM (Deaths)/INZ Deceased Temporary Visa Holders Programme .....	66
14. Citizenship/INZ Entitlement to Reside Programme .....	67
15. Corrections/INZ Prisoners Programme .....	67
16. Customs/IR Child Support Alerts Programme .....	68
17. Customs/IR Student Loan Interest Programme .....	69
18. MSD/IR Working For Families Tax Credits Administration Programme .....	70
19. MSD/IR Working for Families Tax Credits Double Payment Programme .....	71
20. Customs/Justice Fines Defaulters Alerts Programme .....	71
21. INZ/Justice Fines Defaulters Tracing Programme .....	73

# CONTENTS

22. IR/Justice Fines Defaulters Tracing Programme .....	74
23. MSD/Justice Fines Defaulters Tracing Programme .....	75
24. Customs/MED Motor Vehicle Traders Importers Programme .....	76
25. MoT/MED Motor Vehicle Traders Sellers Programme .....	77
26. BDM (Births)/MoE Student Birth Confirmation Programme .....	78
27. BDM (Births)/Ministry of Health NHI and Mortality Register Programme .....	78
28. BDM (Deaths)/Ministry of Health NHI and Mortality Register Programme .....	79
29. ACC/MSD Benefit Eligibility Programme .....	80
30. BDM/MSD Identity Verification Programme .....	80
31. BDM (Deaths)/MSD Deceased Persons Programme .....	81
32. BDM (Marriages)/MSD Married Persons Programme .....	82
33. Centrelink/MSD Change in Circumstances Programme .....	83
34. Centrelink/MSD Periods of Residence Programme .....	84
35. Corrections/MSD Prisoners Programme .....	84
36. Customs/MSD Arrivals and Departures Programme .....	85
37. Customs/MSD Periods of Residence Programme .....	86
38. Educational Institutions/MSD (StudyLink) Loans & Allowances Programme .....	87
39. HNZ/MSD Benefit Eligibility Programme .....	88
40. IR/MSD Commencement/Cessation Benefits Programme .....	89
41. IR/MSD Commencement/Cessation Students Programme .....	90
42. IR/MSD Community Services Card Programme .....	91
43. IR/MSD Debtors Tracing Programme .....	92
44. IR/MSD (Netherlands) Tax Information Programme .....	92
45. Ministry of Education/MSD (StudyLink) Results of Study Programme .....	93
46. Netherlands/MSD Change in Circumstances Programme .....	94
47. Netherlands/MSD General Adjustment Programme .....	94
48. BDM (Deaths)/NPF Eligibility Programme .....	95
49. BDM (Deaths)/NZTA Deceased Driver Licence Holders Programme .....	95
6: FINANCIAL & PERFORMANCE STATEMENTS .....	99
Statement of responsibility .....	99
Audit report .....	100
Statement of objectives and service performance 2009/10 .....	102
Statement of accounting policies for the year ended 30 June 2010 .....	110
Statement specifying comprehensive income .....	119
Statement of comprehensive income for the year ended 30 June 2010 .....	119
Statement of movements in equity for the year ended 30 June 2010 .....	120
Statement of financial position as at 30 June 2010 .....	120
Statement of cash flows for the year ended 30 June 2010 .....	121



# CONTENTS

Statement of commitments as at 30 June 2010 .....	122
Statement of contingent liabilities as at 30 June 2010 .....	122
Notes to the financial statements for the year ended 30 June 2010 .....	123

## Section 3 Tables

TABLE 1: OFFICE OF THE PRIVACY COMMISSIONER WORKPLACE GENDER PROFILE 2009/10 .....	22
TABLE 2: OFFICE OF THE PRIVACY COMMISSIONER WORKPLACE ETHNIC PROFILE 2009/10 .....	22

## Section 4 Tables

TABLE 3: COMPLAINTS RECEIVED AND CLOSED 2005–2010 .....	31
TABLE 4: ACT/CODE – BREAKDOWN OF COMPLAINTS RECEIVED 2009/10 (previous year in brackets) .....	31
TABLE 5: PRINCIPLES/RULES IN COMPLAINTS RECEIVED 2009/10 .....	32
TABLE 6: ACT/CODE – BREAKDOWN OF CLOSED COMPLAINTS 2009/10 (previous year in brackets) .....	33
TABLE 7: PRINCIPLES/RULES IN CLOSED COMPLAINTS 2009/10 .....	33
TABLE 8: AGE OF COMPLAINTS CLOSED 2009/10 (previous year in brackets) .....	35
TABLE 9: OUTCOMES ON CLOSED FILES 2009/10 .....	35
TABLE 10: COMPLAINTS RECEIVED AND CLOSED BY AGENCY TYPE 2009/10 (previous year in brackets) .....	36
TABLE 11: COMPLAINTS RECEIVED AND CLOSED FOR TOP RESPONDENT AGENCIES 2009/10 .....	37
TABLE 12: OUTCOMES FOR TOP RESPONDENT AGENCIES 2009/10 .....	37
TABLE 13: REFERRALS, TRIBUNAL CASES AND OUTCOMES 2004–2010 .....	40

## Section 5 Tables

TABLE 14: FIRST-TIME APPROVALS 2009/10 .....	56
TABLE 15: RENEWED APPROVALS 2009/10 .....	56

## Figures

Figure 1: Total files and files over 12 months old .....	34
Figure 2: Age of complaints in progress as at 30 June 2010 .....	34
Figure 3: Active authorised information matching programmes 2009/10 .....	52
Figure 4: Authorised and active information matching programmes 2002-2010 .....	55

# 1: KEY POINTS

# 1: KEY POINTS

## Information and communications

- We received 7,151 enquiries from members of the public and organisations seeking advice on privacy matters. This number was more than 500 up on 2008/09. Enquiry topics that stood out during the year included Google's collection of WiFi and other data during its Street View activities and New Zealand Post's competition and survey activity.
- Media enquiries have more than doubled over the last two years. In 2007/08 we had 133 media enquiries, last year we had 217 and this year we had 323.
- This year's Privacy Awareness Week, run with our partners from the Asia Pacific Privacy Authorities (APPA) forum, featured a successful one-day conference in Wellington on "The Future of Privacy".
- We formed an advisory group of secondary school students to listen to what they had to say about privacy. Resulting from the students' discussions and work, the group developed material (a brochure, poster and DVD) to be part of an educational kit for secondary schools.
- Our public opinion survey showed high levels of concern about individual privacy and risks to personal information on the internet. The UMR survey also showed a dramatic rise in New Zealanders' use of social networking.
- The Office delivered 35 workshops and seminars to members of the public and stakeholder groups as well as 30 presentations by the Commissioner and staff to a wide range of audiences, such as health and business groups, both in New Zealand and overseas.

## Investigations

- We received 978 complaints, up from 806 last year. This continues an upward trend in complaints.
- 25 percent of complaints were closed by settlement or mediation – an increase from last year. We try to move parties towards settlement, helping them to avoid the expense and stress of court proceedings.
- 97 percent of complaints are under 12 months of age, with 80 percent closed within six months of receipt.

## Policy and technology

- We monitor 49 active government information matching programmes, 29 of which use online data transfers.
- Policy work during the year involved a wide range of projects with central and local government, the private sector, industry bodies and voluntary organisations. Significant areas we have worked on include border control, search and surveillance, and new frameworks for information sharing between government agencies.
- There continue to be significant health information privacy issues around the new National Health IT Plan, shared electronic health records, and governance of national collections of health information and biological material.
- Our follow-up survey on the use of portable storage devices by government agencies showed generally improved security around their use but some key agencies still need to improve their practices.
- We released a proposed amendment to the Credit Reporting Privacy Code inviting submissions from the public. The amendments result from a two year review of the code, which included consulting a reference group of consumer and industry representatives.
- We began an inquiry into Google's collection of information from WiFi networks, to see whether Google's actions breached the Privacy Act and how we might prevent this situation from reoccurring.

## International

- The Office played a key part in two new initiatives: the establishment of the APEC Cross-border Privacy Enforcement Arrangement (CPEA) and the Global Privacy Enforcement Network (GPEA).
- The Office contributed to several international forums including the OECD Working Party on Information Security and Privacy.



# 2: INTRODUCTION

## 2: INTRODUCTION

### **Some headlines from our year**

For a small office, we undertake an unusually wide range of work. The work is both fascinating and challenging.

Some examples are:

- we are handling an increasing number of complaints, enquiries and requests for assistance
- there are some additional challenges to privacy at the moment, with moves towards greater information sharing in government. This is taking up a lot of our time – we are trying to help public sector agencies find more efficient and cheaper ways of conducting their business while also maintaining privacy and the trust of people they deal with
- we are developing some simple tools for small and medium sized businesses to help them manage personal information well
- we are trying to keep track of developing technologies such as geolocation services
- we have an active and important role in international privacy forums.

Throughout this report, we give specific examples of our work. Here are some headlines from our year to illustrate the range of things that we have done.

### **A step towards greater business opportunities**

The Privacy (Cross Border) Amendment Bill (since passed into law) came before the Select Committee at the beginning of July, with strong support from us.

Passing the Bill is a vital step to enable the European Union to white-list New Zealand as a place to which businesses can confidently send personal information, knowing that we have top-class privacy protection. White-list status will give New Zealand businesses a competitive edge internationally and open up new trading opportunities, for example in data processing, cloud computing, and financial or call centre activity.

<http://www.privacy.org.nz/report-by-the-privacy-commissioner-to-the-minister-of-justice-on-the-privacy-cross-border-information-amendment-bill/>

### **Balancing privacy with needs of search and surveillance**

The Select Committee hearings on the Search and Surveillance Bill were held in September. The Bill, by its nature, covers activities that are intrinsically privacy-

invasive such as the power to search people and property, and using new technologies for surveillance.

We took the view that while the Bill was generally sound, it did not always strike the right balance between privacy and other interests. For example, we considered whether subjects of surveillance could be notified of the surveillance (even if only after the event); the need for warrants to be specific when information is collected from remote facilities (like internet storage sites); and the importance of having some processes to safeguard the privacy interests of innocent third parties (such as family members) caught up in surveillance.

The Law Commission did further work on the Bill during the year, including consulting with us and other submitters. We have recently concluded that the revised Bill provides better safeguards for privacy.

<http://www.privacy.org.nz/search-and-surveillance-bill-2009-submission-by-the-privacy-commissioner/>

<http://www.privacy.org.nz/assets/Files/Reports-to-ParlGovt/Second-submission-to-Select-Committee-23-September-2010.doc>

### **Complaints and our role in settlement put to the test**

Our complaint investigation and settlement processes received some publicity during the year, following a high profile disclosure of personal information about two beneficiaries by Social Development Minister, Hon Paula Bennett. The disclosure resulted in a complaint to us by one of the beneficiaries, and we investigated this complaint.

As usual with complaints, we encouraged the parties to see whether they could resolve the complaint in a mutually satisfactory way. However, they were unable to do so.

Since we found that the complaint had substance, we followed our normal process of referring it to the Director of Human Rights Proceedings for his consideration. The Director will decide whether to take proceedings in the Human Rights Review Tribunal.

<http://www.privacy.org.nz/minister-s-disclosure-of-personal-information-media-release/>

<http://www.privacy.org.nz/privacy-commissioner-closes-investigation-about-hon-paula-bennett-refers-matter-to-director-of-proceedings/>

### **Providing guidance for some key groups**

In October, we released guidance material for businesses looking to install CCTV security systems. CCTV is a common technology, but small businesses in particular do not always know how to manage the privacy issues correctly



or have the right CCTV system for their needs. The guidance includes an easy checklist to help businesses get it right.

The guidance has already come into its own, with some local authorities using it to adopt or modify their CCTV systems, and taxi companies considering it when installing security cameras in taxis operating in major centres.

We also published a booklet, *Privacy in Schools*, to help principals, teachers and boards of trustees deal with the privacy issues that schools commonly face.

Our youth advisory group also produced material to help secondary school students to better manage their own privacy.

Finally, we published guidance material for health practitioners dealing with mental health information.

<http://www.privacy.org.nz/privacy-and-cctv-a-guide-to-the-privacy-act-for-businesses-agencies-and-organisations/>

<http://www.privacy.org.nz/media-release-new-privacy-guidance-for-schools/>

<http://www.privacy.org.nz/youth/>

### **An enormous task for the Law Commission – and for us**

During the summer, the Law Commission published two major volumes on privacy. The first was the report on *Invasion of Privacy: Penalties and Remedies* (on reform of such matters as offences and the development of tort law). The second was the issues paper on the Privacy Act itself (*Review of the Privacy Act 1993*).

We have kept in close contact with the Law Commission during its privacy project, and have made submissions on each area. Our submission on the Privacy Act discussion paper attempted to answer every question that the Law Commission had posed. We also provided the Law Commission with an options paper on possible enforcement models that a revised Privacy Act could implement.

<http://www.privacy.org.nz/privacy-commissioner-welcomes-law-commission-review-media-release/>

### **Privacy by design takes a great step forwards**

After suggestions from us, the New Zealand Computer Society has introduced requirements in its new professional standards that IT professionals should build in privacy right at the start of their projects. The standards also mean that IT professionals should have a general understanding of the privacy principles. This should result in a far greater focus on “privacy by design” – not purely as a matter of legal compliance, but because good privacy results in more effective IT systems.

The Commissioner also stressed the need for privacy by design in her keynote speech to the Biometrics Institute conference. Having privacy as a forethought rather than an afterthought avoids the need for costly add-ons, last-minute design changes or consumer backlash from launching a product that does not meet privacy expectations.

<http://www.itcp.co.nz/files/PKCV1.pdf>

<http://www.privacy.org.nz/protecting-biometric-data-privacy-by-design/>

### **Owning up to mistakes**

One of the privacy breaches notified to us this year was ACC's mistaken mail-out of claimant information to the wrong employers.

Every month, around 15,000 businesses get a report from ACC about injuries that have occurred in their workplaces. In February, ACC's external mail-house did not collate all the information correctly. This resulted in approximately 2000 employers receiving information about claimants who were not their employees.

ACC followed our breach notification guidelines, including taking steps to retrieve the reports and get them to the correct businesses, letting the claimants know, checking procedures to prevent recurrence of the incident, and contacting us to let us know about the breach.

<http://www.privacy.org.nz/privacy-breach-guidelines-2/>

### **International commissioners band together**

In 2010, international privacy commissioners started to join forces on breaches of privacy by corporations whose activities affect people in different jurisdictions. Collective action is particularly important for small countries such as New Zealand, whose citizens can only be properly protected if global solutions are found.

In the first example of its type, in April we joined nine other privacy commissioners to write an open letter to Google in response to its faulty launch of the Google Buzz product. Google Buzz was a new social networking service that Google set up for G-Mail users. It identified people's frequent correspondents and automatically assigned users a public network of "followers" from among those correspondents. Google did not properly tell people how the new service would work or that their followers would be visible for anyone to see. There was a significant backlash from the public, and, as a result, Google changed how Buzz worked.

The commissioners urged Google to make sure that fundamental privacy safeguards are incorporated into the design of new services rather than having to address problems after launch. The commissioners used the example of Buzz to remind Google and other international organisations of the need to comply

with the local laws of the countries in which they operate.

International collaboration of this type is likely to increase as new cross-border enforcement initiatives under APEC and the global privacy enforcement network get under way.

<http://www.privacy.org.nz/media-release-privacy-guardians-warn-multinationals-to-respect-laws/>

<http://www.privacy.org.nz/launch-of-new-apec-cross-border-privacy-enforcement-arrangement/>

<http://www.privacy.org.nz/global-privacy-enforcement-network-launches-website/>

### **Getting electronic health records right**

The draft National Health IT Plan, released this year, is an important step in New Zealand's movement towards devising an effective electronic health records system. As in other countries, New Zealand's health agencies are considering ways in which technology can enhance how health information is managed.

An electronic health records system can give both consumers and health providers better access to and control over health information. But such a system needs to be carefully constructed with privacy at the forefront of both the policy and technology decisions. We will continue to be involved as the proposals for the system take greater shape.

<http://www.privacy.org.nz/comments-on-national-health-it-draft-plan/>

### **Moving to more comprehensive credit reporting?**

In June, we released a proposed amendment to the Credit Reporting Privacy Code for public consultation. If the amendment proceeds, among other things it would allow more comprehensive credit reporting in New Zealand, including reporting "positive" information about people.

For some time, we have been considering whether the Credit Reporting Privacy Code still adequately deals with the realities of the credit reporting environment. In particular, it makes sense both for the public and for business for Australia and New Zealand to align the way our laws operate, since our major credit reporters operate both in Australia and New Zealand. Australia is considering making changes to its own credit reporting regulation, including permitting more comprehensive credit reporting.

<http://www.privacy.org.nz/major-changes-to-nz-credit-reporting-regulation-credit-reporting-privacy-code-2004-proposed-amendment-open-for-public-submission/>

# 3: OFFICE & FUNCTIONS OF THE PRIVACY COMMISSIONER

## 3: OFFICE AND FUNCTIONS OF THE PRIVACY COMMISSIONER

### **Independence and competing interests**

The Privacy Commissioner has wide-ranging functions. The Commissioner must have regard to the Privacy Act's information privacy principles and the protection of important human rights and social interests that compete with privacy. Competing social interests include the desirability of a free flow of information and the right of government and business to achieve their objectives in an efficient way. The Commissioner must also take account of New Zealand's international obligations, and consider any general international guidelines that are relevant to improved protection of individual privacy.

The Privacy Commissioner is independent of the Executive. She is free from influence by the Executive when investigating complaints, including those against Ministers or their departments. Independence is also important when examining the privacy implications of proposed new laws and information matching programmes.

### **Complaints**

One of the Privacy Commissioner's key functions is to receive and investigate complaints about interferences with privacy. This process is described in detail in the complaints section of this report.

### **Education and publicity**

Part of the Commissioner's role involves promoting an understanding and acceptance of the information privacy principles. Enquiries officers answer questions from members of the public and maintain an 0800 number so that people may call without charge from anywhere in New Zealand.

The Office maintains a website ([www.privacy.org.nz](http://www.privacy.org.nz)) that contains many resources, including guidelines, case notes, fact sheets, newsletters, speeches and reports.

Staff members give regular workshops and seminars, tailored to the audience, on the Privacy Act, Health Information Privacy Code, security breach guidelines and information matching.

The Commissioner makes public statements on matters affecting privacy, and

the Office responds to many news media enquiries. When speaking publicly, the Commissioner may act as a privacy advocate but also has regard to wider and competing considerations.

## Legislation and policy

One of the Commissioner's most significant roles is to comment on legislative, policy or administrative proposals that impact on the privacy of individuals or classes of individuals. Many recommendations are adopted by government departments, cabinet committees or by select committees when they are considering policy and legislative proposals. In every case, the Commissioner also has due regard for interests that compete with privacy.

Other functions of the Privacy Commissioner include:

- monitoring compliance with the public register privacy principles
- reporting to the Prime Minister on any matter that should be drawn to his attention, particularly the need for and desirability of taking legislative, administrative or other action to give protection, or better protection, to the privacy of the individual.

## Information matching programmes

Another key area of work is in monitoring the growing number of government information matching programmes. These programmes must operate in accordance with the provisions of the Privacy Act.

## Codes of practice

The Privacy Commissioner may issue 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 within a particular industry or sector.

## Functions under other enactments

A range of functions are given to the Privacy Commissioner under enactments other than the Privacy Act. These additional statutory roles usually involve providing specialist input on privacy matters or some form of safeguard or 'watchdog' role. Some statutes require a public agency to consult the Privacy Commissioner when implementing a new statutory scheme in order to allay public concern or avoid privacy 'teething' problems. Some statutes confer a review role or complaints function. This is more cost effective than creating a new review or complaints body, especially when disputes are expected to arise only rarely.

## Reporting

The Privacy Commissioner reports to Parliament through the Minister of Justice, and is accountable as an independent Crown entity under the Crown Entities Act 2004.

## Equal employment opportunities

The Privacy Commissioner has developed and implemented an Equal Opportunities Policy, in line with the advice and guidance provided to Crown entities, to meet her 'good employer' obligations. During the 2009/10 year, the main areas of focus have been:

- reviewing personal and operational policies to provide fair and transparent policies, processes, tools and support for managers, and information for staff
- providing a professional and positive working environment
- making family-friendly practices available to all staff (for example, flexible working hours).

The Commissioner continues to place a strong emphasis on fostering an inclusive culture.

### 3: OFFICE & FUNCTIONS OF THE PRIVACY COMMISSIONER

TABLE 1: OFFICE OF THE PRIVACY COMMISSIONER  
WORKPLACE GENDER PROFILE 2009/10

	Women		Men		Total
	Full-time	Part-time	Full-time	Part-time	
Commissioner	1				1
Senior managers	1		3		4
Team leaders	4				4
Investigating officers	4		2		6
Administrative support	5	2	1		8
Advisers (technology & policy)	2		3		5
Enquiries officers	1		1		2
Total	18	2	10		30

TABLE 2: OFFICE OF THE PRIVACY COMMISSIONER  
WORKPLACE ETHNIC PROFILE 2009/10

	Māori		Pacific Peoples		Asian (including Sth Asian)		Other ethnic groups		Pakeha/ European	
	Full-time	Part-time	Full-time	Part-time	Full-time	Part-time	Full-time	Part-time	Full-time	Part-time
Commissioner									1	
Senior managers									4	
Team leaders									4	
Investigating officers									6	
Administrative support					1				5	2
Advisors (technology & policy)									5	
Enquiries officers									2	



## Staff

The Privacy Commissioner employs staff in the Auckland and Wellington offices.

The Assistant Commissioner (Auckland) is responsible for the areas of law reform, codes of practice, international issues and special projects such as Commissioner initiated inquiries.

The Assistant Commissioner (Legal and Policy) is legal counsel to the Privacy Commissioner, leads and manages litigation and gives advice in the area of investigations. She also manages the Office's communications, policy, technology and information matching work.

The Assistant Commissioner (Investigations) has responsibility for complaints and investigations functions and manages teams of investigating officers in both offices.

A Senior Adviser (Legal and Public Affairs) reports directly to the Commissioner.

The General Manager is responsible for administrative and managerial services to both offices. Administrative support staff are employed in each office.

Contract staff are variously involved in management, accounting and publication work for the Office.

# 4: REPORT ON ACTIVITIES

## 4: REPORT ON ACTIVITIES

### **International activities**

Information and communications technologies are creating an increasingly interconnected world. Technological innovation builds upon and accelerates other forces of globalisation such as free trade, labour mobility and leisure travel. Long gone are many of the old certainties about the processing of personal information being kept within national boundaries. It is increasingly difficult even to know where an individual's personal information is being held.

Although the pace of technological change seems never to slacken, one general trend has been plain to see for many years – that information freely travels about the globe as an integral part of the new economy. Part of this is a drive for efficiency. Equally important is the drive to deliver better services that have led to innovations in business models. Indeed, we now routinely expect products and services that would not have been dreamt of by most consumers a mere decade or so ago.

Much of this innovation and rapid data exchange is great news for individuals, business, government and the economy generally. After all, New Zealand is physically distant from major markets. E-commerce can help to 'level the playing field' in New Zealand's favour for some kinds of trade. However, there are many challenges as well. One of these is the regulatory challenge of protecting personal information consistent with generally agreed international principles and, in New Zealand's case, the Privacy Act 1993.

There are many aspects to these challenges. For example, how can the law ensure that New Zealanders' information is adequately protected when sent offshore for processing? How can our trading partners be sure that their information is safe when sent here for processing? How can New Zealanders exercise their rights of access and correction when information is held in another country? What can be done when an agency's actions breach an individual's privacy?

New Zealanders want their personal information protected wherever it travels. The Office of the Privacy Commissioner can play a useful part in this by engaging effectively with those involved in protecting privacy in other countries and, at the international level, in researching privacy risks and developing coordinated regulatory strategies, standard setting and enforcement cooperation.

For some time, a particular priority for the Office has been to enhance or, in some cases, create mechanisms to promote cooperation amongst privacy enforcement agencies. The year saw two significant milestones in this regard:

the establishment of the APEC Cross-border Privacy Enforcement Arrangement (CPEA) and the Global Privacy Enforcement Network (GPEN). The Office played a part in both developments.

### **Highlights**

#### *APEC Cross-border Privacy Enforcement Arrangement*

APEC Ministers endorsed the APEC Cross-border Privacy Enforcement Arrangement (CPEA) in November 2009. The CPEA focuses on one of the four key goals of the APEC Privacy Framework, namely to facilitate both domestic and international efforts to promote and enforce information privacy protections. The CPEA aims to contribute to consumer confidence in electronic commerce involving cross-border data flows by establishing a framework for regional cooperation in the enforcement of privacy laws.

The Office of the Privacy Commissioner actively participated in the 'Pathfinder initiative' that developed the CPEA, and in the implementation working party that brought the arrangement to fruition in July 2010. This work offers tangible benefits to regulators and consumers, and the Office agreed to be one of four initial co-administrators.

#### *Global Privacy Enforcement Network*

Several years ago, the Office contributed to an OECD working party that developed the OECD Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy. That Recommendation offers a policy blueprint for how countries can individually and collectively create the conditions necessary to facilitate cross-border enforcement of privacy laws. The Recommendation has been influential both in the APEC privacy work and, domestically, in the new complaints-transfer provisions in the Privacy (Cross-border Information) Amendment Bill.

During the year, the Office continued to contribute to work within the OECD that focused on implementation of the Recommendation as well as initial work on reviewing the OECD's 1980 Privacy Guidelines. As part of that work, privacy enforcement authorities from a number of OECD member countries identified the need to establish an enforcement network.

Under the leadership of the US Federal Trade Commission, the Global Privacy Enforcement Network (GPEN) was established. The Office helped to develop that network and was pleased to be one of the 10 founding authorities when GPEN was launched in March 2010. The Office has agreed to assist with the network's administration.

### *Forums*

The Office continued to engage in international activities in a variety of ways including contributing to the following forums:

- Asia Pacific Privacy Authorities (APPA) Forum, which meets twice a year and involves commissioners from Australia, Canada, Hong Kong, Korea and New Zealand. Following decisions taken at APPA during the year, it is likely to include other authorities from throughout the APEC region beginning with the USA
- International Conference of Data Protection and Privacy Commissioners, which brings together more than 80 Privacy Commissioners from around the world in an annual conference, and also involves inter-sessional work through several working groups
- APEC: the Data Privacy Sub-group is APEC's specialist group devoted to privacy policy issues, while CPEA is a network of participating privacy enforcement authorities
- OECD: the Working Party on Information Security and Privacy (WPISP) brings together privacy expertise across OECD countries to advance policy objectives.

## **Information services**

### **Enquiries**

During the 2009/10 year, we received 7,151 enquiries from both members of the public and organisations seeking advice on privacy matters – an increase of around 500 enquiries compared to last year.

Over 80 percent of the enquiries were by telephone. Email contact is increasing and comprised 17 percent of the enquiries.

The Enquiries Team of two people attempts to answer calls live but, failing that, responds within 24 hours to all messages.

Topics that stood out during the year included:

- Google's collection of WiFi and other data during its Street View activities
- New Zealand Post's competition and survey activity
- insurance companies' collection of information.

Collection issues made up 30 percent of the enquiries and questions about disclosure or use of information made up 32 percent.

### **Training and education**

Compared with last year, this was a quieter year for the Office's education work (for which we make a modest cost-recovery charge). We think that the financial downturn played a part in this.

There were 47 workshops and seminars. Most were conducted by the investigations staff with some provided by contractors. As in previous years, there was a high demand for education within the health sector. Courses were delivered in Auckland, Wellington, Christchurch, Nelson, New Plymouth, Rotorua, Wairarapa, Fielding and Palmerston North.

### **Privacy Awareness Week**

For Privacy Awareness Week this year, we held a very successful one-day conference in Wellington on "The Future of Privacy". The conference attracted around 250 participants, including some excellent speakers from New Zealand and overseas. The programme included our youth advisory group's view on privacy and the work it is doing to assist young people; cloud computing; the Law Commission's review of privacy project; electronic health records; and data mining.

We used social media during and after the conference. There were several live Twitter streams during the day, and the presentations from the final panel session "A Picture of the Future" are available on YouTube at [www.youtube.com/PrivacyNZ#](http://www.youtube.com/PrivacyNZ#).

At the international level, the Asia-Pacific privacy commissioners worked together to translate and adapt an online product on ID theft developed by the Norwegian data protection commissioner who made it available to us at no cost. Several New Zealand banks and other agencies have since adopted or promoted the product.

The ID theft product is available at [http://privacyawarenessweek.org/id\\_theft\\_tool/index.html](http://privacyawarenessweek.org/id_theft_tool/index.html)

Other activities during Privacy Awareness Week included our public opinion survey conducted by UMR (<http://www.privacy.org.nz/assets/Files/Surveys/Privacy-survey-2010.pdf>) and an updated survey of how public sector agencies manage portable storage devices (<http://www.privacy.org.nz/assets/Files/Surveys/Portable-Storage-Device-Survey-Report-2010.pdf>).

### **Youth advisory group**

For some time, it has been common to say that young people do not care about their privacy. This is largely because young people are among the highest users

of social media, and often put vast amounts of information about themselves (including some risky information) into the public arena. Rather than relying on popular perceptions, we wanted to find out what young people actually thought about privacy.

We formed an advisory group of secondary school students from the Wellington area, under the guidance of two university students. We listened to what they had to say and then supported them to put their ideas into practice.

Our advisory group told us that young people care a great deal about their privacy but that they are not often aware of steps they can take to protect themselves. They said that three (interlinked) things were important for young people: awareness of what was happening with personal information; the ability to consent; and appropriate use of the information.

The students then worked on advice material for young people. They produced a wallet-sized brochure, a short DVD, a poster, and a kit for schools that provides materials for presenters to use at assemblies and real stories and other resources for teachers or senior students to use in classroom discussions.

The materials are available for free download at [www.privacy.org.nz/youth/](http://www.privacy.org.nz/youth/) and every New Zealand secondary school can get one free kit that brings all the materials together.

#### **Other outreach**

The Commissioner and her senior staff have given a wide range of speeches and presentations during the year. Topics have included:

- protecting biometric data: privacy by design
- credit reporting and privacy
- health privacy in the digital age
- insurers' use of genetic information
- moving towards global regulation of privacy
- developing domestic enforcement practices and strategies
- good privacy practices for RFID
- the impact of the OECD guidelines in NZ
- social media
- privacy for auditors
- portable storage devices.

## Media

The number of media enquiries that we receive has more than doubled over the last two years.

In 2007/08, we had 133 media enquiries, which was a standard number of enquiries for a financial year. Last year, we had 217 enquiries. This year, we had 323.

The rise in media enquiries appears to reflect a growing public awareness and concern about privacy, particularly in relation to information technology. For example, there have been several major stories during the year about the activities of powerful international IT companies such as Facebook and Google. We also regularly get enquiries about use of CCTV security cameras, tracking systems and other surveillance devices. In addition, we had some high-profile complaints during the year that resulted in a flurry of enquiries.

As well as the general rise in interest about privacy, however, no government department currently acts as a leader or spokesperson on information technology and its impacts on individuals. The result is that we have become the natural “go-to” agency for journalists seeking comment, explanations of technology and other assistance.

Even when we do not provide a comment on a particular enquiry, wherever appropriate we try to assist the journalist by giving some background information. However, the number of enquiries we are getting represents a significant amount of high-pressure work for our small office. We increasingly have to be selective, or refer enquiries to others.

## Complaints and access reviews

We received a total of 978 complaints in the 2009/10 year, which is a significant increase from last year’s 806 complaints. For each of the three years prior to that, we had received around 650 complaints.

Table 3 shows incoming and closed complaints, and work in progress at the year’s end. The matters most often complained about have all increased proportionately. Work in progress at the end of the year is within an expected range of between 250 to 350 files.



TABLE 3: COMPLAINTS RECEIVED AND CLOSED 2005-2010

	2005/06	2006/07	2007/08	2008/09	2009/10
Complaints received	636	640	662	806	978
Complaints closed	752	701	767	822	961
Work in progress after year's end	455	394	289	273	290

### Complaints received

Past trends continue to be reflected in the incoming complaints for the year. Of the 978 complaints received, 75 percent were alleged breaches of privacy under the information privacy principles within the Act. Table 4 shows a breakdown between the privacy principles and rules contained in the three codes.

TABLE 4: ACT/CODE – BREAKDOWN OF COMPLAINTS RECEIVED 2009/10 (previous year in brackets)

Act/Code	Number
Privacy Act	734 (659)
Health Information Privacy Code	198 (139)
Telecommunications Privacy Code	11 (1)
Credit Reporting Code	6 (7)
Not identified in category	29 (0)
TOTAL	978 (806)

Table 5 is a breakdown of the principles involved within the complaints received. Individual complaints can mostly be categorised into three broad areas: those where the actions complained of involve collection of personal information; actions involving use or disclosure of personal information; and individuals who seek access to information and in doing so believe that information is incorrect, inaccurate or being withheld unnecessarily.

The first four principles deal with actions involving the collection of personal information. This type of complaint accounted for about 15 percent of our workload. Complainants are often concerned about collections that they were unaware of until they accessed information held by an agency.

Nearly 55 percent of complaints arise from individuals seeking access to personal information held by an agency. Complainants often wish us to review an agency's decision to withhold information. They may have suspicions or evidence that other information ought to be disclosed. They may also be concerned about retention policies or practices.

TABLE 5: PRINCIPLES/RULES IN COMPLAINTS RECEIVED 2009/10

Principle or rule	Number
Purpose for collection	53
Source of information	59
Collection of information	31
Manner of collection	30
Storage of information	67
Access to information	501
Correction of information	85
Accuracy of information	47
Retention of information	14
Use of information	22
Disclosure of information	266
Unique identifier use	1
Charging	9
TOTAL	1,185

Use and disclosure of personal information by an agency resulted in 288 complaints or nearly 25 percent of our workload for the year. Some of these complaints arise out of careless or inadvertent disclosures or uses of information that surprise the person involved. Often, though, people do not fully understand that the agency will use or disclose the information, even when the purpose for collecting the information has been explained to the person.

#### **Complaints closed**

Slightly more than two thirds of the closed complaints for the 2009/10 year involved issues covered by the privacy principles of the Act (see Table 6). The three codes accounted for slightly less than a quarter of the closed files.

TABLE 6: ACT/CODE – BREAKDOWN OF CLOSED COMPLAINTS 2009/10  
(previous year in brackets)

Act/Code	Number
Privacy Act	748 (673)
Health Information Privacy Code	197 (133)
Telecommunications Privacy Code	8 (6)
Credit Reporting Code	8 (10)
TOTAL	961 (822)

As reflected in the received complaint statistics, the majority of complaints closed involved access, use and disclosure issues. The statistics mirror the received complaints. Table 7 shows the overall breakdown.

TABLE 7: PRINCIPLES/RULES IN CLOSED COMPLAINTS 2009/10

Principle or rule	Number
Purpose for collection	53
Source of information	56
Collection of information	32
Manner of collection	27
Storage of information	62
Access to information	503
Correction of information	89
Accuracy of information	54
Retention of information	20
Use of information	20
Disclosure of information	265
Unique identifier use	4
Charging	17
TOTAL	1202

### Age of complaints

At the end of the year, four percent (12 files) of our work in progress was over 12 months old. Two of the files are over two years old because of legal and court challenges about our investigation process. The court cases and subsequent appeals have now been exhausted. The Privacy Commissioner's investigation process was upheld by the courts. Consequently, we hope to conclude these files soon.

Figure 1 shows a month-by-month breakdown of work in progress at the end of each month and the number of files that are more than 12 months old.

Figure 1: Total files and files over 12 months old

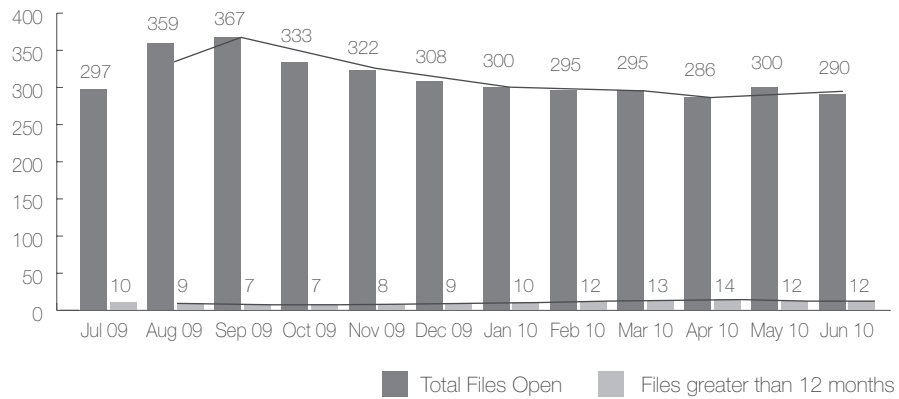


Figure 2 shows the age breakdown of the files held at the end of the year.

Figure 2: Age of complaints in progress as at 30 June 2010

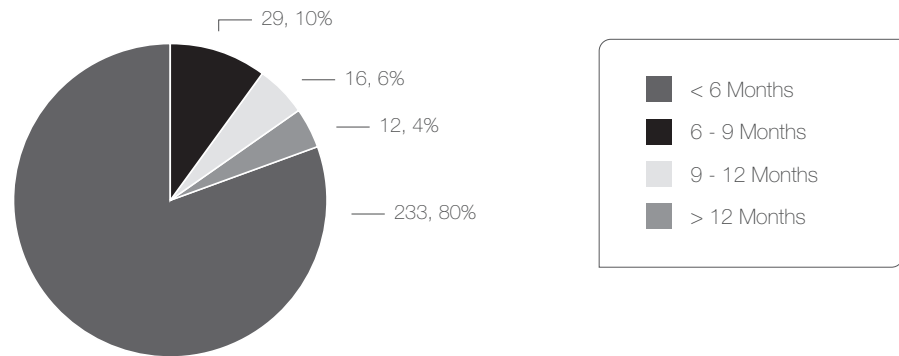


Table 8 shows the age of complaints closed in 2009/10 (previous year in brackets). Our stated intent was to close 80 - 90 percent of our files inside 12 months. We exceeded the desired outcome by closing 97 percent.

TABLE 8: AGE OF COMPLAINTS CLOSED 2009/10  
(previous year in brackets)

Age of complaint	Number closed	Percentage closed*
6 months or less	763 (608)	80% (74%)
6 months to 9 months	128 (103)	13% (13%)
9 months to 1 year	41 (59)	4% (7%)
> 1 year	29 (52)	3% (6%)
TOTAL	961 (822)	(100%)

\*Numbers have been rounded in the percentage column

### Complaint outcomes

Table 9 shows the variety of outcomes on complaints closed during 2009/10. These figures represent an outcome on a file basis.

The emphasis for the office is to motivate parties towards settlement, helping them to avoid the expense and stress of court proceedings. Of the complaints closed, 25 percent were closed by settlement of one form or another.

Not all complaints are amenable to settlement. For example, 29 complaints were withdrawn and a further 94 were not actively pursued by the complainants. Very few of these presented settlement opportunities. In addition, we may take the view that a complaint does not have substance or there is simply no case to answer and, in most cases, we would not promote settlement. However, despite our view that a complaint does not have substance but the parties wish to settle, we will help to facilitate an agreed settlement or outcome.

TABLE 9: OUTCOMES ON CLOSED FILES 2009/10

Withdrawn by complainant	Complainant failed to pursue complaint	Settled/mediated	Interference decision	Referred to Director of Proceedings
29	94	244	69	17

In 69 of our closed complaints we believed that the respondent agency's actions resulted in an interference with the complainant's privacy. In some instances, forming a view that there is an interference with privacy should motivate the respondent to settle the complaint. Also, it will help the parties to understand

our position on a complaint, for instance in case the complaint ends up with the Human Rights Review Tribunal. In some instances, although an interference with privacy may have occurred, we may think the actions or the resulting harm are not serious enough to warrant further action.

Of the 69 interference cases, we referred 18 to the Director of Human Rights Proceedings. Deciding to refer a case involves a number of factors. Having credible and available evidence is one key factor. Others include the seriousness of the breach of the Privacy Act; and the level of harm that occurred as a result of the breach. If a genuine and appropriate offer was made by the respondent agency but not accepted by the complainant, we may decide not to refer. In those cases, where we do not refer the complaint to the Director of Proceedings and settlement has not been achieved, a complainant may file proceedings on their own behalf.

### Agency types

Table 10 provides a breakdown of complaints in various sectors. The numbers of complaints in the reported sectors are very similar to those reported in prior years. All areas have increased in proportion to the general increase in complaints for the year.

TABLE 10: COMPLAINTS RECEIVED AND CLOSED BY AGENCY TYPE  
2009/10 (previous year in brackets)

Agency type	Total	Percentage
Government sector, including education and local authorities	425 (371)	44% (46)
Health sector, including hospitals and medical practices	156 (121)	16% (15)
Financial sector, including banking, insurance, credit agencies and debt collectors	80 (91)	8% (11)
Other	317 (223)	32% (28)
TOTAL	978	100%

### Top respondent agencies

Six agencies were the subject of a significant number of complaints this year. Private sector agencies have not made the "top respondent agency" list for the past two years.

Table 11 sets out the complaints received and the number closed throughout the year for top respondent agencies. In total, these agencies constitute more than a third of the Privacy Commissioner's complaints work, as was the case last year.

TABLE 11: COMPLAINTS RECEIVED AND CLOSED FOR TOP RESPONDENT AGENCIES 2009/10

Agency	Number of complaints received	Number of complaints closed
New Zealand Police	90	98
Ministry of Social Development	55	44
Accident Compensation Corporation	57	57
Department of Corrections	53	54
Department of Labour (Immigration)	44	40
NZ Security Intelligence Service	21	22
TOTAL	320	315

Table 12 shows the various outcomes on the complaints closed for each respondent. There is a noticeable increase in settlement outcomes for all agencies.

TABLE 12: OUTCOMES FOR TOP RESPONDENT AGENCIES 2009/10

Agency	Withdrawn by complainant	Complainant failed to pursue	Settled/mediated	Interference	Referred to Director of Proceedings
New Zealand Police	2	10	18	14	6
Ministry of Social Development	4	8	10	3	0
Accident Compensation Corporation	2	6	14	3	0
Department of Corrections	1	9	16	0	0
Department of Labour (Immigration)	0	5	12	7	1
New Zealand Security Intelligence Service	0	0	0	0	0

All New Zealand Security Intelligence Service cases were progressed to closure by the office. The Privacy Commissioner has oversight of the Service for access and correction issues only. The Service is not subject to our scrutiny under the collection, use or retention principles of the Act. In all cases, the Service was

found to have complied with the Act when managing access requests.

### **Settled complaints**

Of the complaints closed, 244 were settled or mediated. This is an increase over last year's 193.

As in past years, settlement outcomes are variable and differ according to the expectations and willingness of parties to reach consensus. Many access to personal information complaints are settled because the respondent agency accepts the views of the Privacy Commissioner and releases information previously withheld. Often, showing a complainant that a practice will be stopped or changed is sufficient. A genuine apology satisfies many complainants. In addition, a number of complaints involve monetary compensation. This year most monetary settlements were less than \$5,000 but a few were closer to \$10,000.

### **Personal contact and settlement**

Direct personal contact with the parties by our staff appears to increase the potential for settlement outcomes. This year our settlements have increased in number and many settle much earlier than previously. We had personal contact with one or more of the parties to a complaint on 92 percent of the complaint files, compared with 80 percent in 2008/09. This means that for the year, 880 of our closed complaint files involved a conversation with one or more of the parties.

### **Satisfaction survey**

The effectiveness of our complaints processes was also measured by a satisfaction survey during the year. Every complainant and respondent received a satisfaction survey form with our closing letter, along with a prepaid envelope. The survey was completed anonymously.

In brief, the survey seeks comment on overall satisfaction; expectations; whether expectations were met; competence of staff; did staff do what they said they would; were you treated fairly; were individual circumstances taken into account; and was the service good value for taxpayers.

We received 256 survey replies in response, made up of 161 (63 percent) replies from complainants and 95 (37 percent) from respondents. This is a similar rate of return to the previous year. (This is the first full year survey. Last year the survey was undertaken for the last six months of the year.)



The survey results were (last year's survey results in brackets):

- 80 percent (80%) said they were satisfied or very satisfied with the service
- 88.5 percent (93%) had expectations of a good to very good service
- 78.5 percent (77%) felt their expectations were met or exceeded
- 83 percent (83%) agreed or strongly agreed that staff were competent
- 88 percent (90%) agreed or strongly agreed that staff kept their promises
- 78.5 percent (80%) agreed or strongly agreed that they were treated fairly
- 68 percent (71%) agreed or strongly agreed that their individual circumstances were considered
- 75 percent (77%) agreed or strongly agreed that the service was good value for taxpayer money.

The survey results are similar to those in the previous survey. We aim to provide a service where 80 percent or more of the parties rate our service as satisfactory or better.

### **External audit**

We contracted a barrister who is experienced in privacy issues to audit a random selection of 20 closed complaint files to determine the quality of the investigations process. The features assessed were analysis of legal issues, clarity and sensitivity of communications and correspondence, and fairness and timeliness of the process. Each file was awarded points between one and five with five being an excellent overall performance in managing the complaint.

Together, the files scored a total 91 (out of a possible 100 points) with the average file score being 4.55. Nine files scored a maximum five points. This compares favourably with previous audits by the same barrister (in 2006 and 2007) where the overall outcome was 79 and the average 3.95.

## **Litigation**

### **Human Rights Review Tribunal**

If we believe that a complaint has substance and the parties are unable to settle their dispute, we usually refer the complaint to the Director of Human Rights Proceedings. The Director makes an independent decision about whether to take the case to the Human Rights Review Tribunal.

The Tribunal hears proceedings under the Privacy Act as well as the Human Rights Act and the Health and Disability Commissioner Act. Parties can appeal to the High Court from a decision of the Tribunal, and from there can appeal further (on a point of law) to the Court of Appeal and the Supreme Court.

A Privacy Act case can only go to the Tribunal once the Privacy Commissioner has conducted an investigation (however brief). This is to ensure that the parties have a serious chance to resolve the dispute before engaging in litigation.

We referred 18 complaints to the Director during this year. He is still considering whether to file claims in most of those cases. He has filed three claims in the Tribunal during the course of the year, declined to take proceedings in three instances, and has settled two of the complaints.

TABLE 13: REFERRALS, TRIBUNAL CASES AND OUTCOMES 2004-2010

	2004/ 05	2005/ 06	2006/ 07	2007/ 08	2008/ 09	2009/ 10
Referrals to Director	13	12	15	20	12	18
New proceedings	9	17	22	19	29	13
Settled/withdrawn (in HRRT)	4	6	4		3	12
Costs awarded*	-	-	5	5	4	2
Struck out	2	164	2		3	2
No interference	2	5		4	6	5
Interference found	3	5	3	0	1	2

\*costs awarded only recorded since 2006/07

As Table 13 shows, an unusually large number of cases have been filed in the Tribunal and subsequently withdrawn. Some cases have settled before hearing but others have simply been withdrawn. It is unclear why such high numbers have been withdrawn this year, and it is also unclear whether this is an anomaly or a trend. However, it is good that people appear to be finding alternatives to litigation.

The Tribunal has issued seven substantive decisions, that is, decisions where the Tribunal heard the matter in full and found there was either an interference or no interference with privacy. In all but one of these cases, the Tribunal's decision accorded with our opinion during the investigation. The exception involved a complaint about access to information. The Tribunal was sympathetic to the respondent Council in its difficult dealings with the plaintiff but found that it could not withhold the information. As a result, it had interfered with the plaintiff's privacy. However, it refused to give the plaintiff damages as he had suffered no loss as a result.

There was one appeal during the year to the High Court: *Reid v Crown Law Office*.

We appeared at the Court's request as an intervener. The Court agreed with us that a very small amount of additional information could be released to Mr Reid.

### **Judicial review**

We have been involved in two continuing judicial review proceedings this year.

In December, the Court of Appeal delivered its decision in *Jeffries v Privacy Commissioner*, dismissing Mr Jeffries' appeal. Mr Jeffries sought leave to appeal to the Supreme Court. In March, the Court refused to hear an appeal on any of the points that criticised the Privacy Commissioner. It granted leave on a point of general law raised in passing in the Court of Appeal judgement: whether unsolicited communications could be covered by litigation privilege.

The High Court's decision in *Henderson v Privacy Commissioner* in April criticised certain aspects of the Privacy Commissioner's investigation into Dr Henderson's actions. However, the criticisms related to matters that occurred several years ago. We had already proactively changed our procedures to avoid these problems, and so we have not needed to make any further adjustments as a result of the Court's decision.

## **Commissioner initiated inquiries**

### **Google's collection of information from WiFi networks**

In mid-May, we began an inquiry into Google's collection of information from WiFi networks. Our inquiry was well advanced but was not complete within this reporting period.

When it was taking photographs to support its Street View product, Google also collected information about WiFi networks. There were two types of information. First, it collected information that the networks themselves broadcast, such as the name of the network, whether it was secured or unsecured, and the signal strength. This information was deliberately collected to improve the precision of Google's location products. At the time, Google did not inform people that it was collecting the information. This only became apparent several years later.

Second, Google collected small amounts of information crossing unsecured wireless networks at the time its Street View cars were within range. Google has said that: this collection was inadvertent; that it has not used the information and will not do so; that it is securely stored with very limited access; and that it will destroy it on request of the Privacy Commissioner.

We are investigating whether Google's actions breached the Privacy Act and how we might prevent this situation from recurring.

At the same time, we were aware that Google's collection of the content of communications might possibly amount to a criminal offence in New Zealand. Section 80 of the Privacy Act requires the Privacy Commissioner to report to the appropriate authority if there appears to be evidence of a crime or serious misconduct.

We therefore notified the New Zealand Police that our inquiry had revealed the possibility that a crime had occurred; it was for the Police to decide whether an investigation was warranted. The considerations under the criminal law and under privacy law are completely different. This has meant that the Police and we have been able to run our inquiries simultaneously.

## Section 54 authorisations

Section 54 of the Privacy Act allows the Commissioner to authorise actions that would otherwise be a breach of principles 2, 10 or 11, as long as the public interest or the benefit to the individual substantially outweigh the impact on privacy. The power to grant specific exemptions gives the Act extra flexibility by taking account of collections, uses or disclosures of information that are in the public interest, or in the interests of the person concerned.

We have a guidance note for agencies that are considering applying for an authorisation on our website.

We received one application this year, from the Ministry of Health and Department of Labour. The application is on hold, as the Ministry and the Department indicated they might be able to resolve the issue without the need for an exemption.

The application involved section 300 of the new Immigration Act 2009. This section establishes an information matching programme to identify people who are or are not eligible to access publicly funded health and disability support services. That section will come into force on 29 November 2010. In the meantime, the Ministry and the Department wished to start the information matching scheme early, and they applied for a section 54 exemption to allow this.

There is a strong public interest in ensuring that only eligible people have access to publicly funded services. The Ministry estimates that payments for ineligible people currently cost the taxpayer several million dollars per year. Parliament has recognised that an information matching programme is the most effective way to ensure eligibility.

However, the application essentially asked the Privacy Commissioner to bring a legislative provision into effect by a different method from which Parliament had set. Also, we usually grant section 54 exemptions for one-off activities rather

than ongoing activities, although this exemption would only have involved a few months' activity before the legislation came into force. Finally, it appeared that the Ministry and the Department could use interim measures that complied with the Privacy Act and that would deal effectively with some of their concerns.

If there is any delay in the Order in Council process, however, the Ministry and Department may revive their application.

## Policy

Each year, we provide advice to agencies on the potential privacy impacts of a project at varying stages of its life, from initial policy design through to the introduction of legislation or service delivery. Some projects involve ongoing work through the entire process.

Policy work during the 2009/10 year included a wide range of projects with central and local government, the private sector, industry bodies and voluntary organisations. As with 2008/09, the majority of work involved public sector agencies.

Engagement is usually initiated by an agency seeking our input, and our involvement is contributing to an ever-increasing appreciation of privacy issues across government and the private sector.

We have done a lot of work this year to help public sector agencies identify what personal information about their clients they:

- can legally share with other government agencies
- want to share but cannot legally do so.

We have worked with agencies to help them find appropriate ways to share information when it is in the public interest. In some cases, this has been through legislative change, and we have worked with agencies to include additional safeguards to protect the privacy of individuals. An example of this is the sharing of fines information with credit reporters. While we oppose this information sharing in principle, we worked closely with the Ministry of Justice to ensure as many safeguards as possible were included in the policy proposal and the Bill should it proceed.

There has also been a large amount of related work with border sector agencies and their processes for the collection, use and storage of personal information. This has involved extensive engagement with the Department of Labour (Immigration), the New Zealand Customs Service, the Ministry of Agriculture and Forestry, and the Department of Internal Affairs. We are continuing to help agencies to identify impacts on individuals' privacy and to mitigate these while

still responding to the challenges the agencies face.

We have developed new, straightforward guidance materials for agencies, explaining how the Privacy Act applies to their projects and how they can assess and reduce the privacy impacts of their proposals:

<http://www.privacy.org.nz/getting-started/>

### **Health policy**

Health information privacy raises significant issues, particularly in the context of a general international push towards the development of electronic health records. In recognition of this, we have a memorandum of understanding with the Ministry of Health to fund work in the health area. Some notable areas of focus have been: commenting on the draft National Health IT Plan; contributing to a review of the retention and governance of the national 'Guthrie Card' collection; development of and participation in health information consumer and District Health Board privacy officer forums; and developing a memorandum of understanding with the Health and Disability Commissioner to help provide a 'no wrong door' environment for complainants and enquirers.

### **Technology policy**

Major topics that have arisen this year are similar to those in 2008/09. These include: biometrics; video surveillance; portable storage devices; smartcards; ISO standards relating to information technology security and privacy; web-based computing services; and online identity authentication systems. Social networking has been an important new area of focus.

To support this work, we have sought to raise awareness of privacy as it relates to specific technologies through our ongoing series of Technology and Privacy Forums. These free forums attract a diverse audience including people from government, the private sector, industry bodies, academia and the public. The two forums during 2009/10 were held in Wellington to audiences of up to 100 people.

We also initiate our own technology and privacy research projects within the Office. This year, we produced guidance to help agencies manage the personal information they collect when they use closed circuit television (CCTV) cameras.

We repeated our survey of central government agencies about their use of portable storage devices (PSDs). Some key findings of the follow-up survey were: that 69 percent of the agencies surveyed now prohibited the use of personal PSDs for work use (up from 38 percent the year before); that 79 percent of surveyed agencies kept a PSD register (previously 62 percent) and that 76 percent of agencies now use hardware or software controls to limit the use of PSDs (59 percent in 2009).

## Law Commission's review of privacy

The Law Commission has completed the first three stages of its four stage review of privacy. By the end of the reporting period, it was working to complete Stage 4.

The first two stages of the review had established a high level policy overview and addressed public register privacy issues.

The Law Commission completed research and public consultation on Stage 3 during the year. It then released a report making recommendations to improve the adequacy of New Zealand's civil and criminal law to deal with invasions of privacy. The Government's formal response to that report involved delaying most substantive decisions until the completion of Stage 4 of the review.

Stage 4 is a review of the Privacy Act 1993 itself. The Law Commission released a substantial issues paper in March, which posed nearly 200 questions for answer. The Office prepared a very thorough submission answering nearly all questions. At the end of the year, the Law Commission was still analysing the 80 or so submissions it had received.

## Information matching

A large proportion of the technology work we do relates to the Privacy Act's information matching provisions. We provide assistance to agencies that are running – or planning to run – information matching programmes to help them understand the requirements of the Act, and we monitor their compliance with this. As part of this work, we also deliver outreach activities, such as specialist education workshops.

Details of our information matching activities this year, and reports on the 49 active government sector programmes, are in section 5.

## Legislation

Many of the policy projects we are involved in result in draft legislation. We continue to give advice during the drafting process and make submissions to select committees on legislation, if necessary. We are also routinely consulted on bills, regulations, supplementary order papers, and rules at various stages of their development or review.

Legislative work over the reporting year has covered a range of topics. For instance, we recommended to Parliament that it add safeguards to the Border (Customs, Excise and Tariff) Bill so that individuals would always be able to use an alternative to the automated decision process (known as 'Smartgate') at the border. These changes were included in the final legislation.

We also did significant work on comments and submissions about the Search and Surveillance Bill. Our focus was to ensure that any expansion of state powers to gather information – including the power to access electronic information remotely – were appropriately limited and that safeguards were provided while maintaining a pragmatic approach.

### **Codes of practice**

Work on codes of practice during the 2009/10 year has included the ongoing review of the Credit Reporting Privacy Code, including:

- approval and issuing of Amendment No. 3 to the Code and
- public notification of proposed Amendment No. 4 to the Code.

### **Consultations with the Ombudsmen**

The Ombudsmen routinely consult the Privacy Commissioner when information is withheld on privacy grounds under the Official Information Act 1982 or the Local Government Official Information and Meetings Act 1987. Consultation is required by statute.

The decision about whether the agency involved should release information is ultimately one for the Ombudsmen to make since the jurisdiction under the legislation is theirs. However, as the specialist in the privacy arena, the Privacy Commissioner's views are sought on whether it is necessary to withhold information to protect privacy and, if so, whether the public interest is strong enough in the circumstances to outweigh the privacy interest. Where an issue raises generic concerns, or will create an important precedent, the two offices hold more detailed discussions to ensure that all angles are properly canvassed.

During the year, we received 52 consultations from the Ombudsmen and completed and closed 47. This is a more than 100 percent increase on consultations received in the previous year.





# 5: INFORMATION MATCHING

## 5: INFORMATION MATCHING

### Information matching and privacy – an introduction

Information matching (or 'data matching') involves the comparison of one set of records with another, generally with the aim of finding records in both sets that belong to the same person. Matching is commonly used in the public sector to confirm people's eligibility (or continuing eligibility) for a benefit programme, to detect fraud in public assistance programmes or to trace people wanted by the State.

Information matching can be problematic from a privacy perspective because:

- an individual's data can be disclosed without their knowledge
- some of the data disclosed may be incorrect or out of date
- the process of matching two sets of records sometimes produces incorrect matches
- action may be taken against individuals based on incorrect information or incorrect matching
- action may be taken against individuals without their knowledge
- common sense and human judgment may not be used if decisions are automated
- trust and confidence may be eroded if information obtained by one agency is spread to other agencies, combined with other data to create massive datasets or trawled through indiscriminately in the hope of finding some wrongdoing.

The Privacy Act 1993 regulates the practice of information matching in the public sector through the controls in Part 10 of the Act and the rules in Schedule 4.

These controls include:

- ensuring that individuals are aware of the programme and that their information may be included in it (rule 1)
- limiting the disclosure and use of information (rule 4 and the purpose given in the specific statutory provision allowing the programme)
- limiting the retention of information (section 101 and rule 6)
- notifying individuals and allowing them time to challenge the decision before any action is taken (section 103).

## 5: INFORMATION MATCHING

One of the Commissioner's functions is to require government departments to provide reports on their operation of authorised information matching programmes and, in turn, report to Parliament with an outline of each programme and an assessment of each programme's compliance with the Privacy Act. The Commissioner's reports are included in this chapter.

A detailed description of information matching and each active programme can be found on the Privacy Commissioner's website at <http://www.privacy.org.nz/data-matching-introduction>.

## Glossary

The following abbreviations and acronyms are used in this chapter:

ACC	Accident Compensation Corporation
BDM	Registrar of Births, Deaths and Marriages (located within DIA)
Citizenship or DIA(C)	New Zealand Citizenship Office (part of DIA)
Corrections	Department of Corrections
Customs	New Zealand Customs Service
DIA	Department of Internal Affairs
EEC	Electoral Enrolment Centre (a New Zealand Post Group business unit)
GSF	Government Superannuation Fund Authority
HNZ	Housing New Zealand
IMPIA	Information Matching Privacy Impact Assessment
INZ	Immigration New Zealand (a division of the Department of Labour)
IR	Inland Revenue
Justice	Ministry of Justice
MED	Ministry of Economic Development
MoE	Ministry of Education
MoH	Ministry of Health
MoT	Ministry of Transport
MSD	Ministry of Social Development
NHI	National Health Index
NPF	National Provident Fund
NSI	National Student Index
Passports or DIA(P)	New Zealand Passports Office (located within DIA)
RMVT	Registrar of Motor Vehicle Traders
SVB	Sociale Verzekeringsbank (Netherlands)
WfFTC	Working for Families Tax Credits (formerly Family Support Tax Credits)

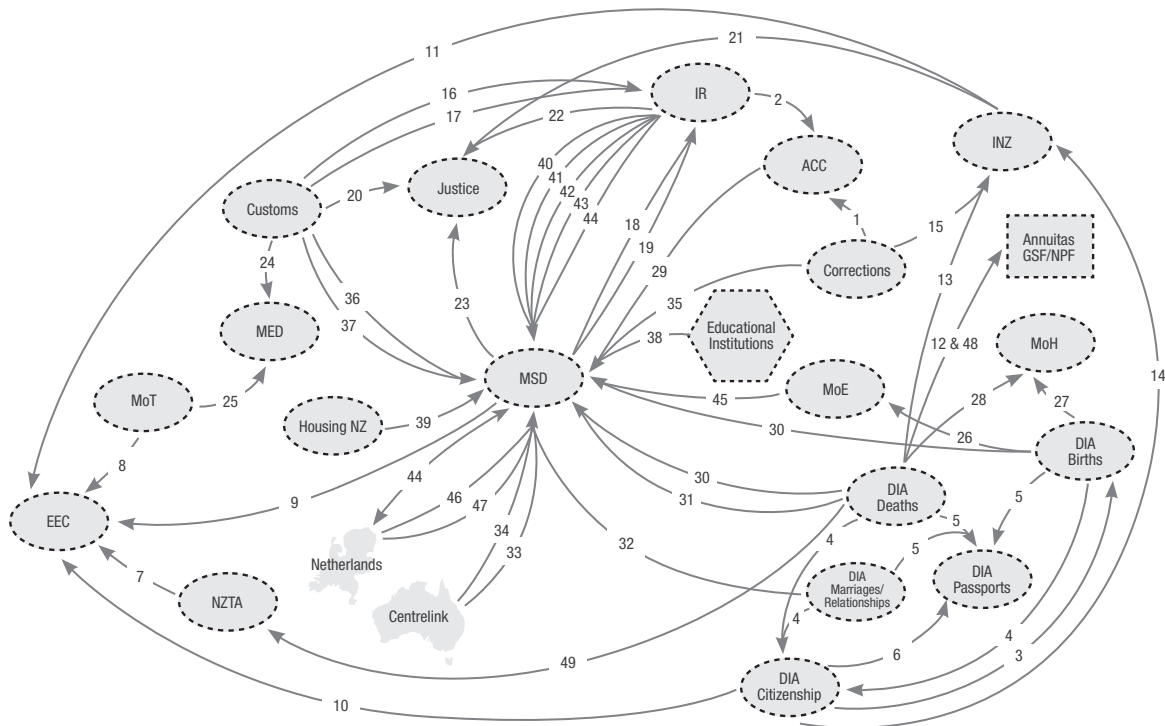
## The year in information matching

Our oversight of information matching during the year included:

- monitoring 49 active programmes
- publishing the fourth edition of our Information Matching Compliance Auditing Information Pack
- reporting to the Minister of Justice on the ability of three new information matching proposals to meet public interest and compliance requirements
- a submission to the Law and Order Select Committee recommending the use of information matching should the Electoral (Disqualification of Convicted Prisoners) Amendment Bill proceed.

Figure 3 shows the flow of information between agencies involved in information matching. An outline of each operating programme and an assessment of its compliance can be found by number in the programme reports later in this chapter.

Figure 3: Active authorised information matching programmes 2009/10



**Highlighted errors***Justice Collection of Fines at Airports (CoFaA)*

In September 2009, changes to the team responsible for managing CoFaA alerts resulted in some reporting and compliance issues for Justice.

Justice cannot conclusively report whether or not fines defaulters were intercepted at the border. This is because Justice staff failed to follow up on missing Police reports which provide the details about which fines defaulters were intercepted (see the Customs/Justice Fines Defaulters Alerts Programme report, page 72).

The new team also did not follow approved processes. Instead of waiting the required five day statutory notice period, Justice staff were immediately releasing information to District Courts where enforcement documents were issued. The result was that several innocent individuals had Court officials visit them and require that they prove their identity on the spot (see the INZ/Justice Fines Defaulters Tracing Programme report, page 73).

Justice has provided the new team with training to ensure it is fully aware of correct procedures, and weekly quality checks have been implemented to ensure that any future issues can be identified promptly.

*IR/MSD Community Services Card Programme*

Inland Revenue identified that it has been under-reporting taxpayer income details to MSD which uses the information to determine eligibility for Community Services Cards. As a result, cards have been issued to an estimated 5,500 people who are not entitled to them.

IR has fixed the data extraction programme used to provide the taxpayer income details. MSD decided not to cancel the cards that have been issued. We will work with IR to identify how the error occurred and to reduce the risk of such errors occurring again (see the IR/MSD Community Services Card Programme report, page 91).

*BDM (Deaths)/NZTA Deceased Driver Licence Holders Programme*

Of 53,680 letters sent as part of a large one-off historical match, NZTA mistakenly sent 421 of those letters before verifying that the details related to the correct person.

NZTA received responses from 23 people who advised that they were not deceased. NZTA decided not to cancel any of the 421 driver licence records (see the BDM (Deaths)/NZTA Deceased Driver Licence Holders Programme report, page 95).

#### *Inland Revenue reporting*

There appeared to be an anomaly in the reported activity for the Customs/IR Student Loan Interest Programme. When questioned, IR found that the programme it uses to generate the statistics had not been updated to include all of the borrower records in the matching process. IR modified its programme to provide the correct figures.

We will work more closely with IR this year to minimise the risk of incorrect reporting. We are also reviewing our overall reporting requirements and the process we use to make our assessment to ensure we are getting the level of detail we need (see the Customs/IR Student Loan Interest Programme report, page 69).

#### **Outreach**

In March, the Office hosted an Information Matching Interest Group meeting for about 20 government sector staff. The Law Commission presented to the group and received valuable feedback on its review of privacy, in particular, its proposals on information matching.

We also published three Information Matching Bulletins during the year. Back copies are available on our website at [www.privacy.org.nz/information-matching-bulletins/](http://www.privacy.org.nz/information-matching-bulletins/).

The Office ran one information matching workshop during the year.

#### **Changes in authorised and operating programmes**

Parliament passed three new information matching authorisations during the year. None of these programmes are active yet. Two of these were part of the Immigration Act (assented 16 November 2009 but an Order in Council, expected in November 2010, is required to bring these into force) and the other was included in the Education Amendment Act (assented 19 May 2010). They are:

- MSD/INZ Sponsorship Obligations Programme
- INZ/MoH Publicly Funded Health Eligibility Programme
- MoE/Teachers Council Unregistered Teachers Programme.

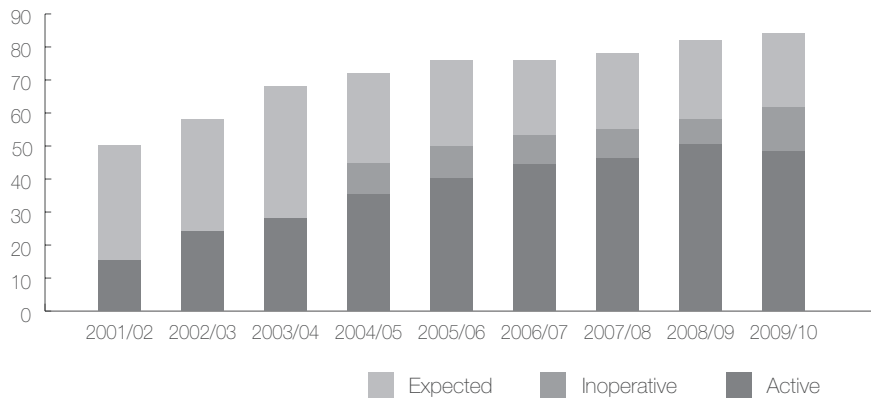
The BDM (Births)/MoE Student Birth Confirmation Programme resumed this year so it has been included in our reporting again.



Three programmes are not reported on as they have not been active this year. They are:

- BDM (Deaths)/Justice (MLC) Maori Land Title Succession Programme
- Netherlands/MSD Debt Recovery Programme
- Employers/MSD Section 11A Social Security Act Programme.

Figure 4: Authorised and active information matching programmes 2002-2010



### Online transfer approvals

The Privacy Act prohibits the transfer of information by online computer connections except with the Commissioner's approval. We grant approvals subject to conditions designed to ensure that agencies put in place appropriate safeguards to protect the data.

The practice of the Office has usually involved granting first-time approvals for 12 months. Based on evidence of safe operation in that first period, and verified by a satisfactory audit report, subsequent approvals are typically issued for a three-year term.

As at 30 June 2010, 29 of the 49 active programmes used online transfers. The 10 requests for online transfers, granted by the Commissioner during the 2009/10 year, are listed below.

TABLE 14: FIRST-TIME APPROVALS 2009/10

User agency Programme name (and number) Approval date	Reason	Grounds
Electoral Enrolment Centre		
Unqualified Voters (programme 11) 28 October 2009	efficiency; data quality	data more current
Teachers Council		
Registration (to operate from 1 July 2010) 22 June 2010	efficiency and security	timely delivery of data

TABLE 15: RENEWED APPROVALS 2009/10

User agency Programme name (and number) Approval date	Reason	Grounds
Department of Internal Affairs (DIA)		
BDM/Passport Eligibility (programme 5) 15 December 2009	continued efficiency; minimisation of data transfer	improved system integration
Citizenship/Passport Eligibility (programme 6) 15 December 2009	continued efficiency; minimisation of data transfer	improved system integration
Inland Revenue		
Working for Families Tax Credits Administration (programme 18) 30 April 2010	continued efficiency	necessary to enable continuous payment of support
Child Support Alerts (programme 16) 17 July 2009	continued efficiency	timely delivery of data; improved system integration
Ministry of Social Development (MSD)		
Commencement/Cessation Benefits and Students (programmes 40 and 41) 21 October 2009	continued efficiency	satisfactory audit result
ACC/Benefit Eligibility (programme 29) 21 October 2009	continued efficiency	satisfactory audit result
Arrivals and Departures (programme 36) 23 December 2009	enhanced verification process	satisfactory operation and clear audit report
New Zealand Transport Agency		
Deceased Driver Licence Holders (programme 49) 8 October 2009	continued efficiency and security	satisfactory operation and clear audit report

## Programme reports

Each entry in the following section begins with a brief description of a programme's purpose and an overview of the information disclosed in the programme. We then report on programme activity, generally in the form of a table of results. Finally, we make an assessment of each programme's compliance with the operational controls and safeguards imposed by ss.99 to 103 of the Privacy Act and the information matching rules.

The reports are presented in alphabetical order based on user agency. The user agency is the second named agency in the programme name. For example, in the BDM/MSD Married Persons Programme, MSD is the user agency.

A detailed description of each active programme, including historical results, can also be found on the Privacy Commissioner's website at [www.privacy.org.nz/operating-programmes](http://www.privacy.org.nz/operating-programmes).

### 1 Corrections/ACC Prisoners Programme

**Purpose:** To ensure that prisoners do not continue to receive earnings-related accident compensation payments.

**Year commenced:** 2000

**Features:** Data is transferred weekly by online transfer.

**Corrections disclosure to ACC:** Corrections provides ACC with the surname, given names, date of birth, gender, date received in prison and any aliases of all people newly admitted to prison.

**2009/10 activity:**

Match runs	44
Records received for matching	83,281
Possible matches identified	1,837
Overpayments established (number)	37
Overpayments established	\$33,028
Average overpayment	\$893
Challenges	0
Challenges successful	0

**Commentary:** Each weekly match run covers prison admissions during the preceding seven days. This year, only 44 match runs occurred because ACC occasionally overlooked the weekly downloading of data extractions. As a result, ACC did not receive all admissions for matching. ACC will request the omitted data to ensure it has examined all admissions.

ACC has centralised the recovery of overpayments because it was concerned about delays in the processing of debts. It advises that this centralisation has resulted in more efficient processing.

**Compliance:** Compliant.

## 2 IR/ACC Levies and Compensation Programme

**Purpose:** To identify ACC levy payers, and to calculate and collect premiums and residual claims levies.

**Year commenced:** 2002

**Features:** Data is transferred weekly by encrypted USB stick.

**IR disclosure to ACC:** For self-employed people, IR provides ACC with the full name, contact details, date of birth, IR number and earnings information. For employers, IR provides ACC with the name, address, IR number and total employee earnings.

**2009/10 activity:**

Self-employed people's records received for matching	774,488
Employers' records received for matching	706,961
Invoices issued to self-employed people	315,112
Invoices issued to employers	584,092
Challenges by individuals	31
Challenges by corporations	56
Total challenges	87
Successful challenges	4

**Compliance:** Compliant.

## 3 Citizenship/BDM Citizenship by Birth Processing Programme

**Purpose:** To enable the Registrar-General to determine the citizenship-by-birth status of a person born in New Zealand on or after 1 January 2006, for the purpose of recording the person's citizenship status on his or her birth registration entry.

**Year commenced:** 2006

**Features:** Data is transferred on request via an online connection.

**BDM disclosure to Citizenship:** For birth registration applications, when no parental birth record can be found, a request is transferred electronically to the Citizenship unit to be manually checked against the relevant citizenship records. The information supplied includes the child's date of birth, parents' full names and birth details.

**Citizenship disclosure to BDM:** Citizenship responds to these requests by stating either the type of qualifying record found or that qualifying records were not found.

**2009/10 activity:**

Births registered	65,575
Notices of adverse action	1,489
Challenges received	310
Successful challenges	175
Citizenship by birth declined	1,314

An audit on the operation of this programme found there were effective controls in place and no significant issues were identified.

**Commentary:** Successful challenges to the accuracy of the matching process are significant at nearly 12 percent, although this is lower than last year's high of 18 percent. This means that more than 150 individuals were initially matched incorrectly as not being eligible for New Zealand citizenship this year. DIA attributes this to instances of incomplete and inaccurate information on some applications that is clarified when the person is contacted.

**Compliance:** Compliant.

## 4 BDM/DIA(C) Citizenship Application Processing Programme

**Purpose:** To verify a parent's citizenship status if required for determining an applicant's eligibility for New Zealand citizenship.

**Year commenced:** 2005

**Features:** Data is transferred on request via an online connection.

**BDM disclosure to Citizenship (DIA):** A computer programme identifies possible matches from the Births, Deaths, Name Change and Marriages (relationships) databases. Only details from these possible matches are displayed to Citizenship staff. These details include full name, gender, birth date, birthplace and parents' full names.

**2009/10 activity:**

Applications for citizenship by descent (may include more than one person)	9,044
Notice of adverse action (arising from failure to match)	5
Successful challenges	4
Citizenship by descent registered	8,373

An audit on the operation of this programme found there were effective controls in place and no significant issues were identified.

**Commentary:** Notices of adverse action are sent when Citizenship cannot satisfactorily match the information supplied to the appropriate birth, death, marriage or relationship record. Almost all of these are resolved by contacting the applicant for clarification.

The difference between the number of applicants and the number registered is primarily due to the applicants not meeting eligibility criteria rather than a failure to correctly match the record.

**Compliance:** Compliant.

## 5 BDM/DIA(P) Passport Eligibility Programme

**Purpose:** To verify, by comparing details with the births, deaths and marriages registers, whether a person is eligible for a passport, and to detect fraudulent applications.

**Year commenced:** 2003

**Features:** Data is transferred on request via an online connection.

**BDM disclosure to Passports (DIA):** A computer programme identifies possible matches from the Births, Deaths and Marriages (relationships) databases. Only details of these possible matches are displayed to Passports staff. These details include full name, gender and date of birth.

**2009/10 activity:**

Passport applications	438,514
Possible matches: Births	1,099,690
Possible matches: Marriages / Relationships	353,981
Possible matches: Deaths	1,453,671
Notice of adverse action	6,596
Successful challenges	6,530
Passports issued (diplomatic, official and standard)	432,889

An audit on the operation of this programme found there were effective controls in place and no significant issues were identified.

**Commentary:** Notices of adverse action are sent when Passports cannot satisfactorily match the information supplied to the appropriate birth, death, marriage or relationship record. Almost all of these are resolved by contacting the applicant for clarification.

The difference between the number of applications and the number of passports issued primarily reflects applications that are still being processed at the end of the period.

**Compliance:** Compliant.

## 6 Citizenship/DIA(P) Passport Eligibility Programme

**Purpose:** To verify a person's eligibility to hold a New Zealand passport from citizenship register information.

**Year commenced:** 2003

**Features:** Data is transferred on request via an online connection.

**Citizenship (DIA) disclosure to Passports (DIA):** A computer programme identifies possible matches from the Citizenship database. The possible matches may involve one or more records. Only details from these possible matches are displayed to Passports staff. These details include full name, date of birth, country of birth and the date that citizenship was granted.

**2009/10 activity:**

Passport applications	438,514
Possible matches to Citizenship records	460,999
Notice of adverse action (arising from failure to match)	694
Successful challenges	687
Passports issued (diplomatic, official and standard)	432,889

An audit on the operation of this programme found there were effective controls in place and no significant issues were identified.

Notices of adverse action are sent when Passports cannot satisfactorily match the information supplied to the appropriate Citizenship record. Almost all of these are resolved by contacting the applicant for clarification.

**Compliance:** Compliant.

## 7 NZTA/EEC Unenrolled Voters Programme

**Purpose:** To compare the driver licence register with the electoral roll to:

- identify people who are qualified to vote but have not enrolled so that they may be invited to enrol
- update the addresses of people whose names are already on the roll.

**Year commenced:** 2002

**Features:** Data transferred on request by CD.

**NZTA disclosure to EEC:** NZTA provides the full name, date of birth and address of driver licence holders aged 17 and over whose records have not been marked confidential.

**2009/10 activity:**

Match runs	5
Records received for matching	1,624,399
Invitations to enrol sent out	197,092
Invitations presumed delivered	184,387
New and updated enrolments	33,014
Percentage of letters delivered resulting in changes	18%
No response	151,373
Cost	\$123,857.89
Average cost per enrolment	\$3.75

**Commentary:** The large number of records received for matching cover a 14-month period. During that time, NZTA cleaned up its address records and these cleaned-up records were provided to EEC as address changes. There was also significant publicity of proposals to increase the driver licence minimum age. This publicity may have prompted people to become licensed, even if they were not directly affected by the age criteria.

**Compliance:** Compliant.

## 8 MoT/EEC Unenrolled Voters Programme

**Purpose:** To compare the motor vehicle register with the electoral roll to:

- identify people who are qualified to vote but have not enrolled so that they may be invited to enrol
- update the addresses of people whose names are already on the roll.



**Year commenced:** 2002

**Features:** Data transferred on request by CD.

**MoT disclosure to EEC:** MoT provides full name, date of birth and address of individuals aged 17 and over who registered a vehicle or updated their details in the period covered by the extraction. The 'Owner ID' reference number is also included to identify any multiple records for the same person.

**2009/10 activity:**

Match runs	5
Records received for matching	2,108,072
Invitations to enrol sent out	175,993
Presumed delivered	167,846
New and updated enrolment	31,529
Percentage of letters delivered resulting in changes	19%
No response	136,317
Cost	\$112,736.78
Average cost per enrolment	\$3.58

**Compliance:** Compliant.

## 9 MSD/EEC Unenrolled Voters Programme

**Purpose:** To compare MSD's beneficiary and student databases with the electoral roll to:

- identify beneficiaries and students who are qualified to vote but who have not enrolled so that they may be invited to enrol
- update the addresses of people whose names are already on the roll (beneficiary records only).

**Year commenced:** 2002

**Features:** Data transferred on request by CD.

**MSD disclosure to EEC:** MSD provides full name, date of birth and address of all individuals aged 17 years or older for whom new records have been created or where key data (surname, given name or address) has changed, provided these records have not been flagged as confidential.

**2009/10 activity:**

Match runs	5
Records received for matching	905,612
Invitations to enrol sent out	174,943
Presumed delivered	170,004
New and updated enrolments	28,862
Percentage of letters delivered resulting in changes	17%
No response	141,142
Cost	\$111,041.25
Average cost per enrolment	\$3.85

**Compliance:** Compliant.

## 10 Citizenship/EEC Unenrolled Voters Programme

**Purpose:** To compare the citizenship register with the electoral roll so that people who are qualified to vote but have not enrolled may be invited to enrol.

**Year commenced:** 2002

Features: Data transferred on request by CD.

**DIA Citizenship disclosure to EEC:** Citizenship provides full name, date of birth and residential address of new citizens aged 17 years and over (by grant or by descent).

**2009/10 activity:**

Match runs	5
Records received for matching	18,232
Invitations to enrol sent out	810
Presumed delivered	796
New and updated enrolments	106
Percentage of letters delivered resulting in changes	13%
No response	690
Cost	\$1,866.92
Average cost per enrolment	\$17.61

**Compliance:** Compliant.

## 11 INZ/EEC Unqualified Voters Programme

**Purpose:** To identify, from immigration records, those on the electoral roll who appear not to meet New Zealand residence requirements<sup>1</sup> so their names may be removed from the roll.

**Year commenced:** 1996

**Features:** Data transferred online daily.

**INZ disclosure to EEC:** Immigration New Zealand provides full names (including aliases), date of birth, address and permit expiry date. The type of permit can be identified because five separate files are received, each relating to a different permit type.

**2009/10 activity:**

	Bulk match (covering 3 June 2009 to 13 February 2010)	Daily matching (from 14 February 2010)
Records received for matching	436,975	353,079
Possible matches identified	587	338
Notice of adverse action sent	587	338
Challenge received	14	17
Successful challenges	6	17
Removals from roll	581	312
Cost	\$21,308	\$9,745
Average cost per removal	\$36.68	\$31.23

**Commentary:** From 14 February 2010, EEC has operated a daily online transfer to identify people who may be ineligible to enrol.

**Compliance:** Compliant.

## 12 BDM (Deaths)/GSF Eligibility Programme

**Purpose:** To identify members or beneficiaries of the Government Superannuation Fund Authority (GSF) who have died.

**Year commenced:** 2009

**Features:** Data transferred by CD every four weeks.

<sup>1</sup> To enrol to vote in elections an individual must be a citizen or permanent resident of New Zealand.

**BDM disclosure to GSF:** BDM provides information from the Deaths Register covering the 12 weeks prior to the extraction date. The death extraction includes full name at birth, full name at death, gender, birth date, death date, place of birth, and number of years lived in New Zealand (if not born in New Zealand).

**2009/10 activity:**

Records received for matching	33,356
Possible matches identified	9,540
Notices of adverse action sent	544
Challenges	4
Successful challenges	4

**Commentary:** This is the first full year of operation as an authorised information matching programme. The four 'challenges' that have occurred during this period were verified as being mis-matches.

**Compliance:** Compliant.

## 13 BDM (Deaths)/INZ Deceased Temporary Visa Holders Programme

**Purpose:** To identify and remove or update the records of people who are deceased from the Immigration New Zealand (INZ) database of overstayers and temporary permit holders.

**Year commenced:** 2007

**Features:** Data transferred by CD every six months.

**BDM disclosure to INZ:** BDM provides information from the Deaths Register covering the six months prior to the extraction date. The death extraction includes full name at birth, full name at death, gender, birth date, death date, country of birth, and number of years lived in New Zealand.

**2009/10 activity:**

Records received for matching	28,959
Possible matches identified	374
Records marked as deceased - overstayer list	121
Records marked as deceased - temporary visa holders' list	68
Total number of records updated as deceased	189

**Compliance:** Compliant.

## 14 Citizenship/INZ Entitlement to Reside Programme

**Purpose:** To identify and remove from the Immigration New Zealand (INZ) overstayer records the names of people who have been granted New Zealand citizenship.

**Year commenced:** 2004

**Features:** Data transferred by CD every six months.

**Citizenship disclosure to INZ:** Citizenship provides information from the Citizenship Register about people who have been granted citizenship. Each record includes full name, gender, date of birth, country of birth and Citizenship person number.

**2009/10 activity:**

Match runs	3
Records received for matching	1,075,685
Possible matches identified	2,468
Number of NZ citizens removed from the overstayer list	387

**Compliance:** Compliant.

## 15 Corrections/INZ Prisoners Programme

**Purpose:** To identify prisoners who fall within the revocation and/or deportation provisions of the Immigration Act 1987 as a result of their criminal convictions, or are subject to removal from the country because their permit to be in New Zealand has expired.

**Year commenced:** 2005

**Features:** Data transferred weekly by online transfer.

**Corrections disclosure to INZ:** Corrections discloses information about all newly admitted prisoners. Each prisoner record includes full name (and known aliases), date and place of birth, gender, prisoner unique identifier, and name of the prison facility. Each prisoner's offence and sentence information is also included.

**INZ disclosure to Corrections:** For prisoners who are subject to removal or deportation orders, and who have no further means of challenging those orders, INZ discloses the full name, date and place of birth, gender, citizenship, prisoner unique identifier, immigration status and details of removal action that INZ intends to take.

**2009/10 activity:**

Match runs	51
Possible matches identified	365
Cases excluded as not being eligible for removal or deportation	314
Notices of adverse action	51
Successful challenges	0
Cases considered for removal or deportation	50
Removals and deportations from NZ at year's end	26

**Commentary:** Changes to the Immigration Act 2009 relating to this programme come into effect in late November 2010. The changes will allow Corrections to disclose offence date and home detention details in the programme.

We reported a discrepancy last year between one individual's sentencing record received from Corrections and the relevant sentencing record held by Police. An investigation by INZ and Corrections has failed to determine the reason for this discrepancy.

Another discrepancy has occurred this year involving differences between Corrections and Police data. One individual identified in the match had a sentence recorded which was inconsistent with the type of offence recorded. INZ checked with Police and found that its offence information relating to the sentence was different to the offence information held by Corrections.

INZ, Corrections, and Police are investigating this latest anomaly. We share INZ's concern about these discrepancies given that both Corrections and Police receive offence information directly from the Justice system.

INZ reports that information to determine identity and eligibility for removal from New Zealand is thoroughly verified and checked against alternative sources before it takes any action against an individual.

We will work with INZ this year to help it identify and fix the cause of these discrepancies.

**Compliance:** Compliant.

## 16 Customs/IR Child Support Alerts Programme

**Purpose:** To identify parents in serious default of their child support liabilities who leave for, or return from, overseas so that IR can take steps to recover the outstanding debt.

**Year commenced:** 2008

**Features:** Data transferred in close to real-time by online transfer.

**IR disclosure to Customs:** IR provides Customs with the full name, date of birth, and IRD number of parents in serious default of their child support liabilities.

**Customs disclosure to IR:** For high-value debtors (and selected other debtors), Customs provides IR with the person's arrival card information. This includes the full name, date of birth, and date, time and direction of travel including New Zealand port and prime overseas port (last port of call for arrivals and first port of call for departures).

**2009/10 activity:**

Possible matches identified	6,042
Arrival cards received for liable parents	1,440
<b>Number of liable parents</b>	<b>1,093</b>
New contact details updated	465
Existing contact details confirmed	160
Contact details not useful	235
Cards illegible or incomplete	178
Cards did not meet the matching criteria	55

An audit on the operation of this programme found that there are effective controls in place and no issues were identified.

**Compliance:** Compliant.

## 17 Customs/IR Student Loan Interest Programme

**Purpose:** To detect student loan borrowers who leave for, or return from, overseas so that IR can administer the student loan scheme and its interest-free conditions.

**Year commenced:** 2007

**Features:** Data transferred in near real-time by online transfer.

**IR disclosure to Customs:** IR provides Customs with the full name, date of birth, and IRD number for student loan borrowers who have a loan of more than \$20.

**Customs disclosure to IR:** For possible matches to borrowers, Customs provides the full name, date of birth, IRD number and date, time and direction of travel.

**2009/10 activity:** There were 384,434 borrower records updated as a result of matching student borrower records with travel movement information held by Customs.

An audit on the operation of this programme found that there are effective controls in place and no issues were identified.

**Commentary:** Last year, IR reported to us that there were 54,400 borrower records updated. For this year, IR initially told us that there were 146,641 borrower records updated. When we queried this figure - it was such a big increase on the previous year – IR checked its system. It found that the process it used had not been updated from its initial testing phase and did not correctly take account of all the borrower records in the actual matching process. IR then modified its process to produce what it believes to be the correct figures for both years.

The corrected number of borrower records updated last year was in fact 352,401 and the number for this year was 384,434.

We will work more closely with IR during the next year to minimise the risk of incorrect reporting occurring in the future. We are also reviewing our overall reporting requirements and the process we use to make our assessment to ensure we are getting the level of detail we need.

**Compliance:** Compliant but reporting issue identified - see commentary.

## 18 MSD/IR Working For Families Tax Credits Administration Programme

**Purpose:** To inform IR of beneficiaries who have commenced paid employment so that IR can deliver Working for Families Tax Credits (WfFTC).

**Year commenced:** 2005

**Features:** Data transferred each week by online transfer.

**MSD disclosure to IR:** MSD selects clients with children in their care who have had a 'trigger event' relating to the cessation or commencement of employment (i.e. a benefit has been granted, resumed, cancelled or suspended).

MSD sends full name, date of birth, income and benefit payment information, and MSD and IRD client numbers for both the primary carer and his or her partner. In addition, MSD provides the primary carer's bank account number, address and contact details. Details of each child's full name and date of birth are also included.

**2009/10 activity:** An audit on the operation of this programme found that there are effective controls in place and no issues were identified.



WfFTC payments distributed by IR and MSD were \$2,797 million, which is \$114 million (4.3%) more than 2008-09. An average weekly payment of \$153 was paid to 201,000 families.

**Compliance:** Compliant.

## 19 MSD/IR Working for Families Tax Credits Double Payment Programme

**Purpose:** To identify individuals who have wrongly received Working for Families Tax Credits (WfFTC) from both MSD and IR.

**Year commenced:** 1995

**Features:** Data transferred up to 26 times per year by USB stick.

**IR disclosure to MSD:** IR provides MSD with the full name, date of birth, address and IRD number of people (and their spouse, if applicable) who are receiving WfFTC payments.

**MSD disclosure to IR:** For the matched records, MSD supplies the IRD number, the date that tax credits payments started and the amount paid.

**2009/10 activity:** An audit on the operation of this programme found that there are effective controls in place and no issues were identified.

WfFTC debt, as a result of over-payment to individuals, has jumped by over 40 percent in the last two years to \$238 million. The increase in WfFTC debt is not a result of the way the programme operates. Over-payment can occur where the estimated annual income used to establish regular payment levels turns out to be less than the actual income earned for the year.

**Compliance:** Compliant.

## 20 Customs/Justice Fines Defaulters Alerts Programme

**Purpose:** To improve the enforcement of fines by identifying serious fines defaulters as they cross New Zealand borders, and to increase voluntary compliance through publicity about the programme targeted at travellers.

**Year commenced:** 2006

**Features:** Data transferred each day by online transfer.

**Justice disclosure to Customs:** Justice provides serious fines defaulter information for inclusion on Customs' 'silent alerts' or 'interception alerts' lists.

Fines defaulters who have interception alerts recorded are those where:

- any amount of reparation is owing and a warrant to arrest (which covers part of the reparation outstanding) has been issued
- court-imposed fines of \$5000 or more are outstanding and a warrant to arrest (which covers part of the court-imposed fines outstanding) has been issued.

Silent alerts are created for fines defaulters who are not subject to an interception alert but have outstanding fines of \$1000 or more, and a warrant to arrest (which covers part of the outstanding court-imposed fines) has been issued.

Each Justice fines defaulter record disclosed includes the full name, date of birth, gender and a fines defaulter unique identifier number.

**Customs disclosure to Justice:** For each alert triggered, Customs supplies the full name, date of birth, gender, nationality and presented passport number, along with details about the intended or just completed travel.

**2009/10 activity:**

Silent alerts triggered	2,035
Individuals subject to silent alerts	1,062
Intercept alerts triggered	97
People intercepted	64
On departure	14
On arrival	50
Incorrect intercepts (estimate - see commentary)	17
Fines had already been paid	1
Wrong person identified by the match	16
Interception not completed (estimate – see commentary)	16
Fines received	\$76,256
Reparation received	\$116,241
Amount under a current time-to-pay arrangement	\$669,609
Remittals/Alternative sentence imposed	\$61,868

**Commentary:** In September 2009, Justice moved the daily recording of interception and silent alerts to a new team. While reviewing results since the handover, Justice uncovered a series of procedural failures. The new team was failing to follow up with Police about the results of interception alerts and was incorrectly recording the outcomes of some alerts.

The failure to follow up with Police about the outcome of interception alerts means that Justice cannot conclusively report whether or not fines defaulters

were intercepted at the border. As a result, the (estimated) number of cases where interceptions were not completed is much higher than last year.

Justice has provided staff members with training to ensure they are fully aware of correct procedures, and weekly quality checks have been implemented to ensure that any future issues can be identified promptly.

**Compliance:** Compliant but procedural issues identified – see commentary.

## 21 INZ/Justice Fines Defaulters Tracing Programme

**Purpose:** To enable the Ministry of Justice to locate people who have outstanding fines in order to enforce payment.

**Year commenced:** 2006

**Features:** Data transferred weekly by online transfer.

**Justice disclosure to INZ:** Justice sends INZ details of serious fines defaulters who have triggered a 'silent' alert as part of the linked Customs/Justice Fines Defaulters Alerts Programme. Each record includes the full name, date of birth, gender, passport number, Justice personal profile number and flight information of the fines defaulter.

**INZ disclosure to Justice:** INZ supplies information contained on the arrival and departure card, which includes full name, date of birth, gender, passport number, nationality, occupation, New Zealand address and date of expected return to New Zealand (in the case of a departing traveller).

### 2009/10 activity:

Records sent to INZ	1,939
Notices of adverse action	784
Successful challenges	1
Payment received for fines	\$285,883
Amounts under a current time-to-pay arrangement	\$616,983
Remittals/Alternative sentence imposed	\$280,954

**Commentary:** Justice has updated the way it calculates the payments received for fines from this programme. This means that this year's payment received figure is significantly lower than previous years. We will be working with Justice this year to further refine reporting for this programme.

In September 2009, Justice moved the daily processing of silent alerts to a new team. The new team did not follow the approved process. Instead of sending individuals a letter and waiting the required five-day notice period to allow individuals time to challenge the contents of the letter (Privacy Act, s.103), Justice

staff immediately released the newly acquired information to District Courts.

The period of non compliance with correct procedure occurred between September 2009 and July 2010. Justice identified 37 individuals who had enforcement documents issued against them during the five-day notice period. The enforcement actions comprised:

- 24 warrants to seize
- five warrants to arrest
- four attachments to benefits or wages
- two reports to a Judge
- one deduction notice
- one summons to a Registrar's hearing.

While executing the warrants to seize, Court officials found that 15 of the 24 addresses provided to them by Justice were the wrong address or the address was invalid. The failure to comply with the notice provision has adversely impacted on several innocent individuals who had Court officials visit them and require that they prove their identity on the spot.

Justice apparently received no communication or challenges after sending the original letters. However, if individuals had been given the opportunity to challenge the match before a warrant was executed, then Justice may have received challenges from some of these people whose information was not correct.

Justice has provided staff members with training to ensure they are fully aware of correct procedures, and weekly quality checks have been implemented to ensure that any future issues can be identified promptly.

**Compliance:** Non compliant – see commentary.

## 22 IR/Justice Fines Defaulters Tracing Programme

**Purpose:** To enable the Ministry of Justice to locate people who have outstanding fines in order to enforce payment.

**Year commenced:** 2002

**Features:** Data transferred up to 12 times a year by CD.

**Justice disclosure to IR:** Justice selects fines defaulters for whom it has been unable to find a current address, and sends the full name, date of birth, and Justice unique identifier number to IR.

**IR disclosure to Justice:** For matched records, IR supplies address and contact details along with the unique identifier information originally provided by Justice.

**2009/10 activity:**

Match runs	3
Records sent for matching	32,152
Possible matches identified	6,421
Notices of adverse action	3,705
Challenges	47
Successful challenges	6
Collection instituted	1,849
Amount paid or settled	\$678,874

**Commentary:** Records sent for matching were 25 percent of 2009 levels. This is because the system used to select records for the match is not recognising all of the records available for matching. Justice is developing a temporary solution to this, and is expecting to implement a permanent solution in 2011.

Staffing shortages and the reallocation of resources due to industrial action also combined to limit information matching activity this year, with the amount paid or settled dwindling to 11 percent of last year's figure (\$5.9m). Justice expects an increase in activity in the next period.

**Compliance:** Compliant.

## 23 MSD/Justice Fines Defaulters Tracing Programme

**Purpose:** To enable the Ministry of Justice to locate people who have outstanding fines in order to enforce payment.

**Year commenced:** 1998

**Features:** Data transferred up to 13 times per year by CD.

**Justice disclosure to MSD:** Justice selects fines defaulters for whom it has been unable to find a current address from other sources (including the IR/ Justice Fines Defaulters Tracing Programme), and sends the full name, date of birth and Justice unique identifier number to MSD.

**MSD disclosure to Justice:** For matched records, MSD supplies the last recorded address it holds, along with the unique identifier information originally provided by Justice.

**2009/10 activity:** There have been no new match runs during the year. In common with the IR tracing programme, activity has been hampered by staffing shortages and reallocated resources due to industrial action. Justice decided to forgo matching with MSD and focus its limited resources on the match with Inland Revenue. Justice expects this programme to recommence in the next period.

**Compliance:** Compliant.

## 24 Customs/MED Motor Vehicle Traders Importers Programme

**Purpose:** To enable the Ministry of Economic Development (MED) to identify people who have imported more than three motor vehicles in a 12-month period and are not registered as motor vehicle traders, and take action if there is a strong case for prosecution.

**Year commenced:** 2004

**Features:** Data transferred quarterly by online transfer.

**Customs disclosure to MED:** Customs provides MED with the full name, address, contact numbers and a Customs unique identifier of all individuals or entities that have imported more than three vehicles within the previous 12 months.

**MED disclosure to Customs:** MED returns the Customs unique identifier number for those individuals or entities that can be excluded from future matching because they are registered or are not required to be registered.

**2009/010 activity:**

Match runs		3
Records received for matching		259
Individuals or entities of interest identified		87
Notices of adverse action sent		122
Successful challenges	Entities: registered under another name	1
	Entities: primary purpose not financial gain	18
Entities referred to the National Enforcement Unit		2
Registrations as a result of notices of adverse action		3

**Compliance:** Compliant.

## 25 MOT/MED Motor Vehicle Traders Sellers Programme

**Purpose:** To enable Ministry of Economic Development (MED) to identify people who have sold more than six motor vehicles in a 12-month period and are not registered as motor vehicle traders.

**Year commenced:** 2003

**Features:** Data transferred quarterly by online transfer.

**MoT disclosure to MED:** Ministry of Transport (MoT) provides MED with the full name, date of birth and address of all individuals or entities who have sold more than six vehicles in a 12-month period.

**MED disclosure to MoT:** MED provides MoT with the full name, date of birth, address and trader unique identifier of new motor vehicle traders so that these traders are excluded from future programme runs.

### 2009/10 activity:

Match runs		3
Records received for matching		1,603
Individuals or entities of interest identified		973
Notices of adverse action sent		422
Successful challenges	Entities: registered under another name	3
	Entities: primary purpose not financial gain	252
Entities referred to the National Enforcement Unit		0
Registrations as a result of notices of adverse action		5

**Commentary:** Of the 973 individuals or entities of interest identified, MED only followed up on 308 of these by sending a notice of adverse action. Notices of adverse action are normally sent to all individuals or entities of interest identified. Another notable result is the large drop in new registrations achieved as a result of the programme. MED has been unable to explain these results because the key staff member involved in the operation of the programme has been on extended sick leave.

We will be following up with MED during the year to see whether these discrepancies recur.

**Compliance:** Compliant but see comments above.

## 26 BDM (Births)/MoE Student Birth Confirmation Programme

**Purpose:** To improve the quality and integrity of data held on the National Student Index (NSI) and reduce compliance costs for students by verifying their details for tertiary education organisations.

**Year commenced:** 2004

**Features:** Data transferred on request on CD.

**BDM disclosure to MoE:** Births, Deaths and Marriages provides records of New Zealand-born citizens who were born during the period requested. The records include full name, date of birth and gender.

### 2009/10 activity:

Birth records from the period:	01/01/1992 - 31/12/2004
Received for matching	754,480
Matched exactly with NSI record (automatically)	411,923
Matched after manual intervention	11,325
Total birth records matched	423,248
Total birth records not matched	331,232
Percentage matched	56%

**Compliance:** Compliant.

## 27 BDM (Births)/Ministry of Health NHI and Mortality Register Programme

**Purpose:** To verify and update information on the National Health Index (NHI) and to compile mortality statistics.

**Year commenced:** 2009

**Features:** Data transferred monthly by email.

**BDM disclosure to MoH:** BDM provides child's names, gender, birth date, birth place, ethnicity, and parents' names, occupations, birth dates, birth places, address(es) and ethnicities. BDM also indicates whether the baby was stillborn.

### 2009/10 activity:

Records received for matching	65,204
Possible matches identified	65,158
Records not matched	46



Possible matches result in the NHI record being verified or updated.

**Commentary:** An online transfer approval was issued effective until 30 June 2011.

**Compliance:** Compliant.

## 28 BDM (Deaths)/Ministry of Health NHI and Mortality Register Programme

**Purpose:** To verify and update information on the National Health Index and to compile mortality statistics.

**Year commenced:** 2009

**Features:** Data transferred monthly on CD.

**BDM disclosure to MoH:** BDM provides full names (including names at birth) address, occupation, ethnicity and gender, date and place of birth, date and place of death, and cause(s) of death.

### 2009/10 activity:

Records received for matching	28,976
Possible matches identified	25,189
Records not matched	3,653
New NHIs allocated	134
Corrections to matches (including matches from previous years)	30

**Commentary:** After completing the authorised matching, MoH retains for a year the full data received to help, when needed, with matching coroner's reports to the Mortality register. As this is a breach of the time limits specified in the Privacy Act 1993, we have suggested that if MoH can adequately justify retaining this information it applies for a s.102 exemption authorising this retention. The practical risk is that MoH will make decisions based upon information that was believed to be accurate when supplied but which may since have been corrected by DIA.

**Compliance:** Not compliant during the period under report.

## 29 ACC/MSD Benefit Eligibility Programme

**Purpose:** To identify individuals whose MSD entitlement may have changed because they are receiving ACC payments.

**Year commenced:** 2005

**Features:** Data transferred each week by online transfer.

**ACC disclosure to MSD:** ACC selects individuals who have:

- claims where there has been no payment made to the claimant for six weeks (in case MSD needs to adjust its payments to make up any shortfall)
- current claims that have continued for two months since the first payment
- current claims that have continued for one year since the first payment.

For these people, ACC provides MSD with the full name (including aliases), date of birth, address, IRD number, ACC claimant identifier, payment start/end dates and payment amounts.

**2009/10 activity:**

New match runs started in the reporting period	
Match runs	52
Records received for matching	2,235,451
Possible matches identified	6,345
All match runs active in the reporting period	
Matches that required no further action	4,651
Notices of adverse action	1,896
Challenges	60
Successful challenges	44
Overpayments established	1,697
Value of overpayments established	\$2,459,048

**Compliance:** Compliant.

## 30 BDM/MSD Identity Verification Programme

**Purpose:** To confirm the validity of birth certificates used by clients when applying for financial assistance, and to verify that clients are not on the NZ Deaths' Register.

**Year commenced:** 2007

**Features:** The programme is operated daily using data transferred by CD every quarter.

**BDM disclosure to MSD:** BDM provides birth and death information covering the period of 90 years prior to the extraction date.

The birth details include the full name, gender, birth date and place, birth registration number and full name of both mother and father. The death details include the full name, gender, birth date, death date, home address, death registration number and spouse's full name.

**2009/10 activity:**

Benefit applications processed	449,566
Possible matches identified	15,033
Matches that required no further action	2,015
Letters advising update of information	1,742
Notices of possible adverse action	62
Challenges	0
Overpayments established	0
Value of overpayments established	0
Cases referred for further investigation	184

**Commentary:** This year, MSD intended to use the DIA Data Validation Service (DVS) to help them verify the results from this programme. However, agreement could not be reached on the terms for use of DVS so this has not been progressed.

The number of cases referred for further investigation has risen sharply this year. This is because MSD now investigates clients who no longer receive a benefit but who did not provide adequate identification at the time an earlier benefit was granted.

**Compliance:** Compliant.

## 31 BDM (Deaths)/MSD Deceased Persons Programme

**Purpose:** To identify current clients who have died so that MSD can cease making payments in a timely manner.

**Year commenced:** 2004

**Features:** Data transferred each week by online transfer.

**BDM disclosure to MSD:** BDM provides death information for the week prior to the extraction date. The death details include the full name, gender, birth date, death date, home address, death registration number and spouse's full name.

**2009/10 activity:**

New match runs started in the reporting period	
Match runs	53
Records received for matching	29,743
Possible matches identified	5,173
All match runs active in the reporting period	
Matches that required no further action	2,785
Notices of adverse action	2,327
Challenges	0
Overpayments established	418
Value of overpayments established	\$307,882

**Compliance:** Compliant.

## 32 BDM (Marriages)/MSD Married Persons Programme

**Purpose:** To identify current clients who have married so that MSD can update client records and reassess their eligibility for benefits and allowances.

**Year commenced:** 2005

**Features:** Data transferred weekly by online transfer.

**BDM disclosure to MSD:** BDM provides marriage information covering the week prior to the extraction date. The marriage details include the full names of each spouse (including name at birth if different from current name), their birth dates and addresses, and registration and marriage dates.

**2009/10 activity:**

New match runs started in the reporting period	
Match runs	53
Records received for matching	23,556
Possible matches identified	3,189
All match runs active in the reporting period	
Matches that required no further action	1,879
Notices of adverse action	1,265
Challenges	6
Successful challenges	3
Overpayments established	427
Value of overpayments established	\$582,416

**Compliance:** Compliant.

### 33 Centrelink/MSD Change in Circumstances Programme

**Purpose:** This match facilitates the transfer of applications for benefits and pensions and advice of change in circumstances between MSD and Centrelink (the Australian Government agency administering social welfare payments).

**Year commenced:** 2002

**Features:** Data transferred daily by online transfer.

**Centrelink disclosure to MSD:** When Australian social welfare records are updated for people noted as having New Zealand social welfare records, Centrelink automatically sends an update to MSD including the full name, marital status, address, bank account, benefit status, residency status, income change, MSD client number and Australian Customer Reference Number.

**MSD disclosure to Centrelink:** MSD automatically sends the same fields of information to Centrelink when New Zealand social welfare records are updated, if the person is noted as having an Australian social welfare record.

**2009/10 activity:**

Changes of information received by MSD from Centrelink	423,592
Notices of adverse action	7,067
Changes of information sent by MSD to Centrelink	214,682

Notices of adverse action include cases identified by the Centrelink/MSD Periods of Residence Programme.

An audit on the operation of this programme concluded that it complied with information matching requirements.

**Commentary:** When checking the figures being reported for this year, MSD identified an error in its report. Because incorrect dates had been entered, MSD was under-reporting the activity for this match. This has now been corrected and restated figures for previous years supplied.

**Compliance:** Compliant.

### 34 Centrelink/MSD Periods of Residence Programme

**Purpose:** To test the accuracy of Australian residency entitlement information provided by applicants for New Zealand benefits and pensions by matching a sample 10 percent of applicants for specified benefits and pensions.

**Year commenced:** 2002

**Features:** Data transferred monthly by online transfer.

**MSD disclosure to Centrelink:** For a random sample of recent applicants for benefits, MSD provides Centrelink (the Australian Government agency administering social welfare payments) the client's full name (including aliases), date of birth, gender, MSD client number and Australian Customer Reference Number.

**Centrelink disclosure to MSD:** Centrelink provides MSD information showing the periods each individual has been resident in Australia, derived from arrival and departure information.

**2009/10 activity:**

Records were sent for matching	8,788
Australian pensions granted	0

Notices of adverse action are recorded under the Centrelink/MSD Change in Circumstances Programme [see programme 33 on page 83].

An audit on the operation of this programme found that there are effective controls in place and no issues were identified.

**Compliance:** Compliant.

### 35 Corrections/MSD Prisoners Programme

**Purpose:** To detect people who are receiving income support payments while imprisoned.

**Year commenced:** 1995

**Features:** Data transferred each day by online transfer.

**Corrections disclosure to MSD:** Each day, all prisoners who are received, on muster or released from prison are included in the extraction file. Details disclosed include the full name (including aliases), date of birth, prisoner unique identifier and prison location, along with incarceration, parole eligibility date and statutory release date.

**2009/10 activity:**

New match runs started in the reporting period	
Match runs	361
Records received for matching	17,123,224
Possible matches identified	15,543
All match runs active in the reporting period	
Matches that required no further action	5,949
Notices of adverse action	9,650
Challenges	4
Successful challenges	2
Overpayments established	3,442
Value of overpayments established	\$437,528

**Compliance:** Compliant.

## 36 Customs/MSD Arrivals and Departures Programme

**Purpose:** To identify current clients who leave for or return from overseas while receiving income support payments.

**Year commenced:** 1992

**Features:** Data transferred each week by online transfer.

**Customs disclosure to MSD:** Customs provides arrival and departure information covering the week prior to the extraction date. Each travel movement record includes the traveller's full name, date of birth, gender, travel document number, country code and flight details.

**2009/10 activity:**

New match runs started in the reporting period	
Match runs	52
Records received for matching	9,356,667
Possible matches identified	62,119
All match runs active in the reporting period	
Matches that required no further action	34,433
Notices of adverse action	27,632
Challenges	222
Successful challenges	172
Overpayments established	12,228
Value of overpayments established	\$9,011,609

**Commentary:** The programme was updated in July 2009 to identify clients who have different “allowable days out of the country” entitlements. For example, the eligibility for a disability allowance ceases after 28 days absence whereas superannuitants may be out of New Zealand for up to six months before their superannuation entitlement is affected.

Prior to the changes, supplementary assistance (like disability allowance) was only checked if the “out of country” entitlement was exceeded for the core benefit. The enhanced checking of entitlement dates has contributed towards a significant increase in the number of matches identified and the number and value of overpayments established this year.

**Compliance:** Compliant.

### 37 Customs/MSD Periods of Residence Programme

**Purpose:** To enable MSD to confirm periods of residence in New Zealand or overseas.

**Year commenced:** 2002

**Features:** Data accessed online as required for individual enquiries.

**Customs disclosure to MSD:** Customs provides MSD access to its CusMod system for verification of departure and arrival dates.

**2009/10 activity:** MSD staff accessed 482 Customs records.

Two audits of this programme were conducted. Each audit had a different purpose but the scopes of the audits overlapped.

Customs conducted an audit for assurance that MSD was meeting the conditions under which Customs allows access to the CusMod system. This audit identified particular problems with the record keeping not being correctly done by MSD staff. These omissions were a breach of the conditions agreed by Customs and MSD.

Subsequently, MSD completed an audit on the operation of this programme. This audit includes the MSD management responses to fix the problems identified by the Customs audit.

**Commentary:** The auditors found that the actual use of the online access was appropriate but also found that the record keeping needed improvement for the match to be compliant with the agreed conditions. MSD advises that the required improvements were made during the period.

**Compliance:** Not compliant – see commentary.



## 38 Educational Institutions/MSD (StudyLink) Loans and Allowances Programme

**Purpose:** To provide MSD with the enrolment information it needs to assess a student's entitlement to a student allowance, student loan or both. In particular, the information derived from this programme enables MSD to:

- verify that a student is undertaking a programme of study that has been approved by the Tertiary Education Commission
- determine whether the student is full time or part time
- confirm start and end dates of the student's study programme
- confirm any vacation periods exceeding three weeks during the student's period of study
- identify compulsory tuition fees payable from a loan account to an institution.

**Year commenced:** 1998 (allowances); 1999 (loans)

**Features:** Online transfers are used for the bulk of the data. Requests are faxed to institutions which have not developed systems to handle batches of data appropriately.

**MSD StudyLink's disclosure to educational institutions:** When requesting verification of student course enrolments, MSD StudyLink provides the appropriate educational institution the student's full name, date of birth, MSD client number and student ID number.

**Educational institutions' disclosure to MSD StudyLink:** The educational institutions return to MSD StudyLink the student's enrolled name, date of birth, MSD client number, student ID number and study details.

### 2009/10 activity:

Educational institutions involved in the matching programme	657
Records sent for matching	957,562
Individual applicants involved in matching	234,222
Notices of adverse action sent out (individuals may receive more than one)	47,450
Percentage of applicants issued a notice of adverse action	20%
Challenges	202
Successful challenges	96
Decisions to decline loan/allowance	25,060

The percentage figure overstates the percentage of applicants who receive notices of adverse action because some applicants received more than one notice.

**Commentary:** The increase in educational institutions involved in this programme is due to a rise in the number of secondary schools involved.

On the expiry of the online transfer approval, a new approval was granted for a one-year period rather than the usual three years. This short period is to allow sufficient time for MSD StudyLink to complete its rewrite of the information matching agreement with the educational institutions and the associated technical standards report.

**Compliance:** Compliant.

### 39 HNZ/MSD Benefit Eligibility Programme

**Purpose:** To enable MSD to detect:

- 'double-dipping' for accommodation assistance
- differences in information concerning personal relationships, dependent children and tenant income
- forwarding address details for MSD debtors who have left HNZ properties.

**Year commenced:** 2006

**Features:** Data transferred each week by online transfer.

**HNZ disclosure to MSD:** HNZ selects records relating to new tenancies, annual rent reviews, change in circumstance rent reviews and tenancy vacations.

Each record includes the tenant's full name (including aliases), date of birth, MSD client number (if held), income (including income from any boarders), relationship details (to other tenants) and details of any dependants. Also included are details about the property location, tenancy start/end dates, weekly rental charges and any forwarding address provided on termination of the tenancy.

**2009/10 activity:**

New match runs started in the reporting period	
Match runs	52
Records received for matching	91,276
Possible matches identified	6,777
All match runs active in the reporting period	
Matches that required no further action	6,494
Notices of adverse action	108
Challenges	0
Overpayments established	44
Value of overpayments established	\$58,143

**Compliance:** Compliant.

## 40 IR/MSD Commencement/Cessation Benefits Programme

**Purpose:** To identify individuals receiving a benefit and working at the same time.

**Year commenced:** 1993

**Features:** Data is transferred online up to six times per year. A maximum of 100,000 records are allowed per supply.

**MSD disclosure to IR:** MSD clients selected for the programme are those who:

- had stopped receiving a benefit in the period since the last match
- had cancelled benefits included in the previous match run but for whom IR did not return any employment details
- were nominated because of some suspicion
- were included by random selection.

Each record provided to IR includes the surname, first initial, date of birth, IRD number and MSD client number, and benefit date information.

**IR disclosure to MSD:** For the matched records, IR returns the employee's full name, date of birth, MSD client number and IRD number, employer's name, address, email and phone contact details, and employment commencement and cessation dates.

### 2009/10 activity:

New match runs started in the reporting period	
Match runs	6
Records sent for matching	291,588
Possible matches identified	53,978
All match runs active in the reporting period	
Matches that required no further action	20,396
Notices of adverse action	33,859
Challenges	1,846
Successful challenges	345
Overpayments established	7,870
Value of overpayments established	\$10,006,453

**Commentary:** Records sent for matching doubled from September 2009 to 40,000 per match run to help MSD identify overpayments sooner. This resulted in an increase in overpayments established. The number of challenges appears high but the vast majority are of a minor nature relating to small differences in employment period dates.

**Compliance:** Compliant.

## 41 IRD/MSD Commencement/Cessation Students Programme

**Purpose:** To identify individuals receiving a student allowance and working at the same time.

**Year commenced:** 2005

**Features:** Data is transferred online every month except December. A maximum of 50,000 records is allowed per supply.

**MSD disclosure to IR:** MSD randomly selects 5000 records each month relating to students who have been paid an allowance within a specified study period. Each record includes the surname, first initial, date of birth, IRD number and MSD client number, and allowance date information.

**IR disclosure to MSD:** For the matched records, IR provides MSD with the employee's full name, date of birth, IRD number and MSD client number, employer's name, address, email and phone contact details, and employment commencement and cessation dates.

### 2009/10 activity:

New match runs started in the reporting period	
Match runs	11
Records sent for matching	57,978
Possible matches identified	28,283
All match runs active in the reporting period	
Matches that required no further action	7,998
Notices of adverse action	20,613
Challenges	1,244
Successful challenges	479
Overpayments established	7,099
Value of overpayments established	\$5,351,051

**Commentary:** The proportion of successful challenges has doubled since last year. MSD has suggested that this increase was caused by a change in reporting as some customer contacts may not have been identified as challenges in the past. MSD provided refresher training to its data matching officers last year on what is and what is not a challenge.

A review of a sample of challenges received over the year showed the vast majority of challenges are of a minor nature relating to small differences in employment period dates.

**Compliance:** Compliant.

## 42 IR/MSD Community Services Card Programme

**Purpose:** To identify people who qualify for a Community Services Card (CSC) by virtue of their level of income and number of children, thus entitling them to subsidised health care. The match is also used to confirm continuing eligibility of card holders so that automatic renewals can be arranged.

**Year commenced:** 1992

**Features:** Data transferred fortnightly by USB stick.

**IR disclosure to MSD:** For individual taxpayers who have received Working for Families Tax Credits (WfFTC), IR provides MSD with the full name, address, annual income and IRD number of the primary carer (and partner, if any), the number of children in their care and dates of birth, and the annual amount of WfFTC.

### 2009/10 activity:

Match runs	50
Records received for matching	1,548,824
CSCs automatically renewed	226,741
'Invitation to Apply' forms sent out	90,482
Notices of adverse action	22,126
Challenges	80
Challenges successful	65

**Commentary:** IR recently identified two errors in the programme it uses to extract the data for this match. These errors resulted in IR under-reporting income to MSD, which relied upon this information when assessing eligibility for the CSC. As a result, MSD estimated that up to 6,300 cards are currently issued to people who are not entitled to them.

IR has now fixed the data extraction programme, and because the WfFTC rates were changed on 1 October 2010, corrected income figures for all recipients have since been provided to MSD.

MSD has compared the new income information to the eligibility threshold for the CSC to identify those who are eligible for cards and those who currently have cards but are no longer eligible.

MSD writes to everyone who no longer qualifies for the CSC to give them the opportunity to correct any mistakes in the match. Since 1 October, 2010 MSD has written to 7,986 people. Based upon previous year's numbers, MSD would have expected to write to approximately 2,500 people after a change to the rates. This suggests that 5,500 people may have benefited from the errors in IR's data extraction programme. Cards are issued with an expiry date of 30 September, so card holders who are no longer eligible will continue to benefit from the card until it expires on 30 September 2011.

We will work with IR during the next year to identify how the error occurred and what measures it will put in place to minimise the risk of such errors occurring in the future.

**Compliance:** Compliant with the information matching rules but not conforming to the purpose of the programme.

### 43 IR/MSD Debtors Tracing Programme

**Purpose:** To provide contact details of debtors with whom MSD has lost contact to enable MSD to recover benefit overpayments.

**Year commenced:** 1994

**Features:** Data is transferred every two months by USB stick.

**MSD disclosure to IR:** MSD provides IR with the full name, date of birth, MSD client number and IRD number of the debtors that MSD wants to locate.

**IR disclosure to MSD:** IR provides MSD with the person's address, or employer's name, address and telephone number.

**2009/10 activity:**

Match runs	6
Records sent for matching	183,812
Matches potentially useable	59,198
Notices of adverse action	2,369
Debt pursued	\$9,954,002
Repayments received by 30 June of reporting year	\$191,515
Total variable costs incurred	\$73,535

**Compliance:** Compliant.

### 44 IR/MSD (Netherlands) Tax Information Programme

**Purpose:** To enable income information about New Zealand-resident clients of the Netherlands government insurance agencies to be passed to the Netherlands for income testing.

**Year commenced:** 2003

**Features:** Data provided manually as required.

**IR disclosure to Netherlands:** For New Zealand-resident clients of the Netherlands government insurance agencies, IR provides the individual's contact details and income information to the Netherlands Sociale Verzekeringsbank

(social insurance) or Uitvoeringsinstituut Werknemers Verzekeringen (employee insurance). MSD acts as liaison, forwarding valid requests to IR and forwarding the response to the Netherlands.

**2009/10 activity:** One request for information was received and forwarded to IR, and the subsequent response passed back to the Netherlands.

**Commentary:** An audit on the operation of this programme found that there are effective controls in place and no issues were identified.

**Compliance:** Compliant.

## 45 Ministry of Education/MSD (StudyLink) Results of Study Programme

**Purpose:** To determine eligibility for student loans and/or allowance by verifying students' study results.

**Year commenced:** 2006

**Features:** Data is transferred daily by online transfers.

**MSD StudyLink disclosure to MoE:** StudyLink provides MoE with the student's name(s) (in abbreviated form), date of birth, IRD number, study start and end dates, known education provider(s) used by this student and student ID number.

**MoE disclosure to MSD StudyLink:** MoE returns to StudyLink information showing all providers and courses used by the student, course dates, course equivalent full-time student rating and course completion code.

**2009/10 activity:**

Records sent for matching	78,425
Individual applications involved in matching	55,857
Notices of adverse action sent out	4,596
Successful challenges	1,439

While the number of successful challenges appears high, the rate is a similar proportion to previous years. The challenges include corrections to reporting of study history and claims of exemptions that apply to students as well as challenges to the accuracy of the matching process.

On the expiry of the online transfer approval, a new approval was granted for a one-year period rather than the usual three years. This short period is to allow sufficient time for MSD StudyLink to complete its rewrite of the information matching agreement with the MoE and the associated technical standards report.

**Compliance:** Compliant.

## 46 Netherlands/MSD Change in Circumstances Programme

**Purpose:** To enable the transfer of applications for benefits and pensions and advice of changes in circumstances between New Zealand and the Netherlands.

**Year commenced:** 2003

**Features:** Manual transfer of completed application forms as required.

**MSD disclosure to Netherlands:** MSD forwards the appropriate application forms to the Netherlands Sociale Verzekeringsbank (SVB). The forms include details such as the full names, dates of birth, addresses and MSD client reference numbers.

**Netherlands disclosure to MSD:** SVB responds with the SVB reference number.

**2009/10 activity:** As an indicator of activity, MSD issued 207 notices of adverse action. This figure includes some corrections to SVB reference numbers. There were no challenges to these notices.

**Commentary:** An audit on the operation of this programme concluded that it complies with the requirements.

**Compliance:** Compliant

## 47 Netherlands/MSD General Adjustment Programme

**Purpose:** To enable the processing of general adjustments to benefit rates for individuals receiving pensions from both New Zealand and the Netherlands.

**Year commenced:** 2003

**Features:** Data transferred four times each year by CD.

**MSD disclosure to Netherlands:** For MSD clients in receipt of both New Zealand and Netherlands pensions, MSD provides the Netherlands Sociale Verzekeringsbank (SVB) with the changed superannuation payment information, the MSD client reference number and the Netherlands unique identifier.

**Netherlands disclosure to MSD:** SVB advises adjustments to payment rates and the 'holiday pay' bonus.

**2009/10 activity:** MSD made deductions from pension payments to 3,536 people. There were 1,119 MSD clients resident in the Netherlands.

**Commentary:** An audit on the operation of this programme concluded that it complies with the requirements.

**Compliance:** Compliant.



## 48 BDM (Deaths)/NPF Eligibility Programme

**Purpose:** To identify members or beneficiaries of the National Provident Fund who have died.

**Year commenced:** 2009

**Features:** Data transferred every four weeks by CD.

**BDM disclosure to NPF:** BDM provides information from the Deaths Register covering the 12 weeks prior to the extraction date. The death extraction includes full name at birth, full name at death, gender, birth date, death date, place of birth, and number of years lived in New Zealand (if not born in New Zealand).

**2009/10 activity:**

Records received for matching	33,441
Possible matches identified – Pensioners	503
Possible matches identified – Contributors	552
Notices of adverse action sent	1,055
Challenges	1
Successful challenges	1

**Commentary:** This is the first full year of operation as an authorised information matching programme. The one challenge that occurred during this period was verified as involving a mismatch.

**Compliance:** Compliant

## 49 BDM (Deaths)/NZTA Deceased Driver Licence Holders Programme

**Purpose:** To improve the quality and integrity of data held on the Driver Licence Register by identifying licence holders who have died.

**Year commenced:** 2008

**Features:** Data transferred each fortnight by online transfer.

**BDM disclosure to NZTA:** BDM provides death information for the fortnight prior to the extraction date. The death details include the full name (current and at birth), gender, date and place of birth, date of death, home address and death registration number.

**2009/10 activity:*****Fortnightly match runs***

Match runs	26
Records received for matching	28,787
Possible matched identified	18,306
Notices of adverse action	12,319
Challenges	1
Successful challenges	1
Courtesy letters sent	3,669
Driver licence records cancelled	16,268

***Historical match run***

Match runs	1
Records received for matching	600,023
Possible matches identified	236,501
Notices of adverse action	53,680
Challenges	23
Successful challenges	23
Driver licence records cancelled	216,582

**Commentary:** While processing the historical match results, 421 of the 18,660 partially matched records (where a death record was similar but not an exact match with a driver licence record) were not checked by staff prior to notices of adverse action being sent out. The historical match run involved death records for the period 1 January 1987 to 30 September 2008.

NZTA staff attempted to make contact and apologise to those who were sent the letter in error but only a small number of people were able to be contacted. Of the 421 notices sent, NZTA received responses from 23 people who advised that they were not deceased. NZTA decided to take no action to cancel any of the 421 driver licence records.

NZTA is confident this type of error will not recur in the fortnightly programme because the process to sort the results into partial- and exact-matched records is automated. The error during the historic match run came about because this sorting process was completed manually, and in one instance was overlooked. NZTA also advises that the checking processes for the ongoing match are more stringent than those used in the one-off historical match run, and the comparatively small size of the fortnightly file also makes processing much easier. No processing issues have been identified for the fortnightly match runs.

**Compliance:** Compliant but see comments above.



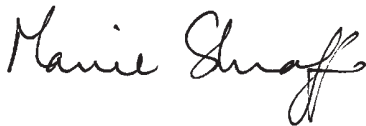
# 6: FINANCIAL & PERFORMANCE STATEMENTS

## STATEMENT OF RESPONSIBILITY

In terms of the Crown Entities Act 2004, the Privacy Commissioner is responsible for the preparation of the financial statements and statement of service performance, and for the judgements made in them.

The Privacy Commissioner has the responsibility for establishing, and has established, 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, these financial statements and statement of service performance fairly reflect the financial position and operations of the Privacy Commissioner for the year ended 30 June 2010.



**Privacy Commissioner**

M Shroff

29 October 2010



**General Manager**

G F Bulog

29 October 2010

## Audit Report

TO THE READERS OF THE OFFICE OF THE PRIVACY COMMISSIONER'S FINANCIAL STATEMENTS AND STATEMENT OF SERVICE PERFORMANCE FOR THE YEAR ENDED 30 JUNE 2010

The Auditor-General is the auditor of the Office of the Privacy Commissioner (the Privacy Commissioner). The Auditor-General has appointed me, John Scott, using the staff and resources of Audit New Zealand, to carry out the audit on her behalf. The audit covers the financial statements and statement of service performance included in the annual report of the Privacy Commissioner for the year ended 30 June 2010.

### Unqualified opinion

In our opinion:

- The financial statements of the Privacy Commissioner on pages 110 to 135:
  - comply with generally accepted accounting practice in New Zealand
  - fairly reflect:
    - the Privacy Commissioner's financial position as at 30 June 2010; and
    - the results of its operations and cash flows for the year ended on that date.
- The statement of service performance of the Privacy Commissioner on pages 102 to 109:
  - complies with generally accepted accounting practice in New Zealand; and
  - fairly reflects for each class of outputs:
    - its standards of delivery performance achieved, as compared with the forecast standards outlined in the statement of forecast service performance adopted at the start of the financial year; and
    - its actual revenue earned and output expenses incurred, as compared with the forecast revenues and output expenses outlined in the statement of forecast service performance adopted at the start of the financial year.

The audit was completed on 30 October 2010, and is the date at which our opinion is expressed.

The basis of our opinion is explained below. In addition, we outline the responsibilities of the Privacy Commissioner and the Auditor, and explain our independence.

### Basis of opinion

We carried out the audit in accordance with the Auditor-General's Auditing Standards, which incorporate the New Zealand Auditing Standards.

We planned and performed the audit to obtain all the information and explanations we considered necessary in order to obtain reasonable assurance that the financial statements and statement of service performance did not have material misstatements, whether caused by fraud or error.

Material misstatements are differences or omissions of amounts and disclosures that would affect a reader's overall understanding of the financial statements and statement of service performance. If we had found material misstatements that were not corrected, we would have referred to them in our opinion.

The audit involved performing procedures to test the information presented in the financial statements and statement of service performance. We assessed the results of

those procedures in forming our opinion.

Audit procedures generally include:

- determining whether significant financial and management controls are working and can be relied on to produce complete and accurate data;
- verifying samples of transactions and account balances;
- performing analyses to identify anomalies in the reported data;
- reviewing significant estimates and judgements made by the Privacy Commissioner;
- confirming year-end balances;
- determining whether accounting policies are appropriate and consistently applied; and
- determining whether all financial statement and statement of service performance disclosures are adequate.

We did not examine every transaction, nor do we guarantee complete accuracy of the financial statements and statement of service performance.

We evaluated the overall adequacy of the presentation of information in the financial statements and statement of service performance. We obtained all the information and explanations we required to support our opinion above.

#### **Responsibilities of the Privacy Commissioner and the Auditor**

The Privacy Commissioner is responsible for preparing the financial statements and statement of service performance in accordance with generally accepted accounting practice in New Zealand. The financial statements must fairly reflect the financial position of the Privacy Commissioner as at 30 June 2010 and the results of its operations and cash flows for the year ended on that date. The statement of service performance must fairly reflect, for each class of outputs, the Privacy Commissioner's standards of delivery performance achieved and revenue earned and expenses incurred, as compared with the forecast standards, revenue and expenses adopted at the start of the financial year. The Privacy Commissioner's responsibilities arise from the Crown Entities Act 2004.

We are responsible for expressing an independent opinion on the financial statements and statement of service performance and reporting that opinion to you. This responsibility arises from section 15 of the Public Audit Act 2001 and the Crown Entities Act 2004.

#### **Independence**

When carrying out the audit we followed the independence requirements of the Auditor General, which incorporate the independence requirements of the New Zealand Institute of Chartered Accountants.

Other than the audit, we have no relationship with or interests in the Privacy Commissioner.



John Scott  
Audit New Zealand  
On behalf of the Auditor-General, Auckland, New Zealand

# STATEMENT OF OBJECTIVES AND SERVICE PERFORMANCE 2009/10

## Output 1 – Privacy Policy

Provide advice on the privacy impact of proposed legislation and other significant proposals.

Monitor and advise on international developments, new technologies and other issues affecting privacy.

Assess proposals for information matching, monitor and report on authorised information matching programmes and review statutory authorities for information matching.

Quantity	Achievement
Contribute to the Law Commission's review of privacy	Achieved. Attended 6 of the monthly meetings held by the Law Commission. Filed one submission to the Law Commission.
Issue and keep current codes of practice	Achieved. Reviewed the Credit Reporting Privacy Code.
Provide practical advice to departments on privacy issues and fair information practices arising in proposed legislation and in administrative proposals	Achieved. The Office provided advice to government departments on 126 occasions across a variety of issues.
Provide specialised assistance to government departments in accordance with agreed memoranda of understanding	Achieved. Policy Adviser (Health) position continued under the MOU with the Ministry of Health has proved highly successful. Progress achieved on the Work-plan (created under the MOU) monitored through quarterly Progress Reports and Progress Meetings held between the Ministry of Health and the Office of the Privacy Commissioner.  In accordance with the MOU with the Department of Internal Affairs, specialised assistance and advice was provided to the Department when requested.



Provide assistance to improve whole-of-government compliance with information matching controls	<p>Achieved.</p> <p>The Privacy Commissioner granted two new information matching files.</p> <p>Monitored 49 active matches.</p> <p>Produced three Information Matching Bulletins and undertook two information matching workshops.</p>
Contribute to international initiatives to facilitate cross-border co-operation in privacy standard setting and enforcement	<p>Achieved.</p> <p>Attended APEC and OECD meetings.</p> <p>Attended accountability meetings (Paris) to progress New Zealand accreditation by the European Union.</p> <p>Founding member of Global Privacy Enforcement Network.</p>

Activities	Estimation	Achieved
Information matching workshops	1	2
Technology and Policy forums	4	2

Quality	Achievement
All proposals for codes of practice will be the subject of discussion with stakeholders and a public submission process which includes a clear statement of purpose	<p>Achieved.</p> <p>Established the Credit Reporting Privacy Code Reference Group to review the Code.</p> <p>Sought public submission into review of the Code through advertising in Public Notices of major print media.</p>
All issued codes are referred to the Regulations Review Committee of the House of Representatives	<p>Not Achieved.</p> <p>The Code was issued prior to referral to the Regulations Review Committee.</p>
Assistance provided to government agencies presents a clear, concise and logical argument, with assumptions made explicit and supported by facts	<p>Achieved.</p> <p>Provided advice and assistance to government agencies, in particular Ministry of Health, Ministry of Social Development, Department of Internal Affairs and the State Service Commission.</p> <p>Evidenced through continuation of Memorandum of Understanding with Departments following reviews of activities for previous year.</p>

Respond to feedback obtained from recipients of policy advice	<p>Achieved.</p> <p>The development of policy and legislation is an iterative process, and any one project may involve several rounds of comments and meetings between the relevant agency and the Office. A key part of the task for the Office is gaining a clear understanding of the objectives an agency is seeking and the policy justifications for those goals.</p> <p>Feedback is also achieved in the regular meetings held with the agencies for which we have an active MOU.</p>
---	--

Timeliness	Achievement
Codes of practice meet the agreed timelines for release and implementation	<p>Achieved.</p> <p>Issued Credit Reporting Privacy Code Amendment #3(CRPC) within the agreed timeline being 30 June 2010.</p>
Advice given within a time span that will enable it to be useful to the recipient or within agreed internal timeframes	<p>Achieved.</p> <p>Timeframes consistently met, even when short notice from agency.</p>

## Output 2 – Information and Outreach

Implement our outreach programme across all activities of the Office to support and promote:

- awareness and understanding of and compliance with the Privacy Act and
- awareness of privacy rights and issues, and an appreciation of privacy as a human right.

Quantity	Achievement
Organise New Zealand Privacy Awareness Week as part of Asia-Pacific Privacy Awareness Week	<p>Achieved.</p> <p>Privacy Awareness Week ran from 2-9 May, in conjunction with other Asia-Pacific Privacy Authority members.</p>

Undertake speaking engagements	<p>Achieved.</p> <p>The Commissioner and her staff provided 30 formal speaking engagements and were involved in a wide number of informal engagements involving community groups and special interest groups on a less formal basis.</p>
Respond to media enquiries	<p>Achieved.</p> <p>The Office responded to 323 media enquiries, up from 200 in the previous year.</p>
Provide assistance to promote better privacy practice in the development of policy and legislation and administrative practices by government agencies	<p>Achieved.</p> <p>Began development of new privacy advice material.</p> <p>Conducted a workshop on this material at the Privacy Forum in May 2010.</p>
Contribute to the Law Commission Privacy Review	<p>Achieved.</p> <p>Attended 6 of the monthly meetings held by the Law Commission.</p> <p>Filed one submission to the Law Commission</p>
Participate in international forums	<p>Achieved.</p> <p>Active participation in the Asia-Pacific Privacy Authority (APPA) communicators' network, particularly over Privacy Awareness Week but also information about other communications initiatives.</p> <p>We are participants in the international network of Privacy Commissioners' communications staff.</p>
Support, where appropriate, networking by agency privacy officers, to develop and improve their effectiveness	<p>Achieved.</p> <p>We provide a venue for Wellington "Privacy Officers Round Table" (PORT) and participate when invited.</p> <p>Privacy Officer portal on website to improve interaction and support with Privacy Officers.</p>
Undertake a programme of education workshops to promote awareness and understanding of, and compliance with, the Privacy Act	<p>Achieved.</p> <p>The Office conducted 47 workshops in this financial year, either on its own premises or visiting individual agencies. This includes workshops out of Auckland and Wellington.</p>

Provide a free enquiries service including 0800 helpline and website access to information, supporting self-resolution of complaints	Achieved. The Enquiries line is operated by two staff who fielded over 7000 calls and contacts during this financial year.
Maintain an effective website and other publications to assist stakeholders to promote better privacy practice	Achieved. The website gives clear, plain English information about privacy, rights and obligations under the law, and the work of the Office. The website is constantly maintained and new information is added within a week of becoming available (usually within 24 hours).
Commission an independent survey of public opinion to measure privacy awareness and the range of attitudes to privacy within the community	Achieved. An independent public survey was undertaken by UMR Research and released in May 2010.

Activities	Estimation	Achieved
Education workshops	40	47
Presentations at conferences / seminars	10	c.30
Projected number of enquiries received and answered	6,000	7000+
Case notes produced	10	12
Media enquiries	150	323

Quality	Achievement
Meet internal professional standards	Achieved. External feedback consistently very positive.
Act on feedback obtained from recipients of advice	Achieved. Always willing to act on feedback. No particular examples this year.
Evaluations show that the expectations of 90% of attendees at workshops were either met or exceeded for quality of presentation and materials	Achieved. All workshops undertaken by the Office are formally evaluated and are of consistently high standard with evaluations showing that expectations of attendees were met or exceeded in over 97% of instances.

Publications and information are legally accurate	Achieved. Publications and website information approved by Assistant Commissioner Legal and Policy as being legally accurate prior to publication or uploading.
Case notes conform to regional standards adopted by the Asia Pacific Privacy Authorities (APPA)	Achieved. Comply with the citation standard as set by Asia-Pacific Privacy Authority (APPA).
Meetings held with or presentations made to at least 10 significant privacy interest groups	Achieved. The Privacy Commissioner or her staff undertook 26 presentations to privacy interest groups.
Reliable and relevant information is placed on the website	Achieved. The website is regularly updated. Information to be placed on the website is quality checked to ensure it is legally accurate and relevant for publication on the site.
Enquiries are answered by appropriately trained professional staff	Achieved. Both staff are fully trained and are experienced.

Timeliness	Achievement
Workshop timetables published on the website	Achieved. Two six monthly timetables are published on our website.
Current information is placed on the website within a fortnight of being made available	Achieved. Information usually placed on website same day it is available; if staff not immediately available then within 48 hours.
Response times to enquiries meet internal standards	Achieved. Staff are able to answer a proportion of calls live, and other enquiries are answered within the working day that they are received.  We attempt to return all unanswered calls within 24 hours.

## Output 3 – Compliance

Handle complaints of interference with privacy.

Enhance cooperation between privacy regulators internationally.

Undertake Commissioner Initiated Investigations (CIIs) as required.

Monitor active information matching programmes.

Quantity	Estimation	Achieved
Number of complaints received	600	978
Number of current complaints processed to completion or settled or discontinued	600	961
Projected number of active information matching programmes monitored	50	49

Quality	Achievement
Complainants' and respondents' satisfaction with the complaints handling process rated as "satisfactory" or better in 80% of responses to a survey of complaints received and closed in the preceding period	Achieved.  Survey of both complainants and respondents conducted throughout the year. The survey measured our endeavours to keep in touch with the parties, understanding of communications from this office, outcomes, value for taxpayer money and overall complaint handling satisfaction.  Overall 80% of those who replied felt the process was satisfactory or better.
When a Human Rights Review Tribunal case is concluded, the outcome will be reviewed against the work of the office with the findings reported to the Privacy Commissioner	Achieved.  Cases assessed in Management Team Meeting as part of the monthly report by Assistant Commissioner Legal and Policy.
External review is conducted of a sample of complaints investigations for their standard of the legal analysis, correctness of the legal conclusions, soundness of the investigative procedure and timeliness	Achieved.  External audit of 20 randomly selected complaint files. Overall the files collectively scored 90 (previous year 91) out of a possible 100 points, the average being 4.5. Ten files scored a maximum 5. This compares favourably with previous audits by the same Barrister (2006 and 2007) where the overall outcome was 79 and the average 3.95.

Referrals to the Director of Proceedings meet expected standards of evidential sufficiency and public interest in all cases	Achieved. Director only occasionally declines to take cases. No instances where he has declined because we should not have referred that matter to him.
Reports to be published on operating information matching programmes will be submitted to relevant departments for comment before publication	Achieved. Reports are submitted to relevant departments prior to publication in the annual report.
<b>Timeliness</b>	<b>Achievement</b>
80-90% of complaints are completed, settled or discontinued within 12 months of receipt	Achieved. 97% of complaints were completed, settled or discontinued within 12 months of receipt.
A report on all operating information matching programmes will be provided annually	Achieved. A report on all authorised information matching programmes is provided in the Annual Report of the Office of the Privacy Commissioner.

# STATEMENT OF ACCOUNTING POLICIES

**FOR THE YEAR ENDED 30 JUNE 2010**

## **Reporting entity**

These are the financial statements of the Privacy Commissioner, a Crown entity in terms of the Public Finance Act 1989 and the Crown Entities Act 2004. As such the Privacy Commissioner's ultimate parent is the New Zealand Crown.

These financial statements have been prepared in accordance with the Public Finance Act 1989.

In addition, the Privacy Commissioner has reported the funding administered on behalf of the Crown as notes to the financial statements.

The Privacy Commissioner's primary objective is to provide public services to the NZ public, as opposed to that of making a financial return.

Accordingly, the Privacy Commissioner has designated itself as a public benefit entity for the purposes of New Zealand Equivalents to International Financial Reporting Standards ("NZ IFRS").

The financial statements for the Privacy Commissioner are for the year ended 30 June 2010, and were approved by the Commissioner on 29 October 2010. The financial statements cannot be altered after they have been authorised for issue.

## **Basis of preparation**

### **Statement of Compliance**

The financial statements of the Privacy Commissioner have been prepared in accordance with the requirements of the Crown Entities Act 2004, which includes the requirement to comply with New Zealand generally accepted accounting practice ("NZ GAAP").

The financial statements comply with NZ IFRSs, and other applicable Financial Reporting Standards, as appropriate for public benefit entities.

### **Measurement base**

The financial statements have been prepared on an historical cost basis.

### **Functional and presentation currency**

The financial statements are presented in New Zealand dollars and all values are rounded to the nearest thousand dollars (\$'000). The functional currency of the Privacy Commissioner is New Zealand dollars.



**Significant Accounting policies**

The following particular accounting policies which materially affect the measurement of comprehensive income and financial position have been applied:

**Budget figures**

The budget figures are those approved 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 Privacy Commissioner for the preparation of the financial statements.

**Revenue**

Revenue is measured at the fair value of consideration received or receivable.

**Revenue from the Crown**

The Privacy Commissioner is primarily funded through revenue received from the Crown, which is restricted in its use for the purpose of the Privacy Commissioner meeting its objectives as specified in the statement of intent.

Revenue from the Crown is recognised as revenue when earned and is reported in the financial period to which it relates.

**Other grants**

Non-government grants are recognised as revenue when they become receivable unless there is an obligation to return the funds if conditions of the grant are not met. If there is such an obligation the grants are initially recorded as grants received in advance, and recognised as revenue when conditions of the grant are satisfied.

**Interest**

Interest income is recognised using the effective interest method. Interest income on an impaired financial asset is recognised using the original effective interest rate.

**Sale of publications**

Sales of publications are recognised when the product is sold to the customer.

**Rental Income**

Lease receipts under an operating sub-lease are recognised as revenue on a straight-line basis over the lease term.

**Provision of services**

Revenue derived through the provision of services to third parties is recognised in proportion to the stage of completion at the balance sheet date. The stage of completion is assessed by reference to surveys of work performed.

## **Leases**

### **Operating leases**

Leases where the lessor effectively retains substantially all the risks and benefits of ownership of the leased items are classified as operating leases. Operating lease expenses are recognised on a straight-line basis over the term of the lease.

### **Goods and Services Tax (GST)**

All items in the financial statements presented are exclusive of GST, with the exception of accounts receivable and accounts payable which are presented on a GST inclusive basis. Where GST is irrecoverable as an input tax, then it is recognised as part of the related asset or expense.

The net amount of GST recoverable from, or payable to, the Inland Revenue Department (IRD) is included as part of receivables or payables in the statement of financial position.

The net GST paid to, or received from the IRD, including the GST relating to investing and financing activities, is classified as an operating cash flow in the statement of cash flows.

Commitments and contingencies are disclosed exclusive of GST.

### **Income Tax**

The Privacy Commissioner is a public authority for tax purposes and therefore exempt from income tax.

### **Cash and cash equivalents**

Cash and cash equivalents include cash on hand, deposits held at call with banks both domestic and international, other short-term, highly liquid investments, with original maturities of three months or less and bank overdrafts.

### **Debtors and other receivables**

Debtors and other receivables are initially measured at fair value and subsequently measured at amortised cost using the effective interest method, less any provision for impairment.

Impairment of a receivable is established when there is objective evidence that the Privacy Commissioner will not be able to collect amounts due according to the original terms of the receivable. Significant financial difficulties of the debtor, probability that the debtor will enter into bankruptcy, and default in payments are considered indicators that the debtor is impaired. The amount of the impairment is the difference between the asset's carrying amount and the present value of estimated future cash flows, discounted using the original effective interest rate. The carrying amount of the asset is reduced through the use of an allowance account, and the amount of the loss is recognised in the statement of comprehensive income. When the receivable is uncollectible, it is written off against the allowance account for receivables. Overdue receivables that have been renegotiated are reclassified as current (i.e. not past due).

### **Inventories**

Inventories held for distribution, or consumption in the provision of services, that are not issued on a commercial basis are measured at the lower of cost (calculated using the weighted average cost method) and current replacement cost. Where inventories are acquired at no cost or for nominal consideration, the cost is the current replacement cost at the date of acquisition.

The replacement cost of the economic benefits or service potential of inventory held for distribution reflects any obsolescence or any other impairment.

Inventories held for sale or use in the production of goods and services on a commercial basis are valued at the lower of cost and net realisable value. The cost of purchased inventory is determined using the weighted average cost method.

The write-down from cost to current replacement cost or net realisable value is recognised in the statement of comprehensive income in the period when the write-down occurs.

### **Property, plant and equipment**

Property, plant and equipment asset classes consist of land, buildings, leasehold improvements, furniture and office equipment, and motor vehicles.

Property, plant and equipment are shown at cost or valuation, less any accumulated depreciation and impairment losses.

### **Revaluations**

The Privacy Commissioner has not performed any revaluations of property, plant or equipment.

### **Depreciation**

Depreciation is provided on a straight line basis on all property, plant and equipment, at a rate which will write off the cost (or valuation) of the assets to their estimated residual value over their useful lives.

The useful lives and associated depreciation rates of major classes of assets have been estimated as follows:

Furniture and fittings	5 - 7 years
Computer equipment	4 years
Office equipment	5 years

### **Additions**

The cost of an item of property, plant and equipment is recognised as an asset only when it is probable that future economic benefits or service potential associated with the

item will flow to the Privacy Commissioner and the cost of the item can be measured reliably.

Where an asset is acquired at no cost, or for a nominal cost, it is recognised at fair value when control over the asset is obtained.

### **Disposals**

Gains and losses on disposals are determined by comparing the proceeds with the carrying amount of the asset. Gains and losses on disposals are included in the statement of comprehensive income.

When revalued assets are sold, the amounts included in revaluation reserves in respect of those assets are transferred to general funds.

### **Subsequent costs**

Costs incurred subsequent to initial acquisition are capitalised only when it is probable that future economic benefits or service potential associated with the item will flow to the Privacy Commissioner and the cost of the item can be measured reliably.

The costs of day-to-day servicing of property, plant and equipment are recognised in the statement of comprehensive income as they are incurred.

### **Intangible assets**

#### **Software acquisition**

Acquired computer software licenses are capitalised on the basis of the costs incurred to acquire and bring to use the specific software.

Staff training costs are recognised as an expense when incurred.

Costs associated with maintaining computer software are recognised as an expense when incurred.

Costs associated with the development and maintenance of the Privacy Commissioner's website are recognised as an expense when incurred.

#### **Amortisation**

The carrying value of an intangible asset with a finite life is amortised on a straight-line basis over its useful life. Amortisation begins when the asset is available for use and ceases at the date that the asset is derecognised. The amortisation charge for each period is recognised in statement of comprehensive income.

The useful lives and associated amortisation rates of major classes of intangible assets have been estimated as follows:

Acquired computer software	4 years	25%
----------------------------	---------	-----

**Impairment of non-financial assets**

Property, plant and equipment and intangible assets that have a finite useful life are reviewed for impairment whenever events or changes in circumstances indicate that the carrying amount may not be recoverable. An impairment loss is recognised for the amount by which the asset's carrying amount exceeds its recoverable amount. The recoverable amount is the higher of an asset's fair value less costs to sell and value in use.

Value in use is depreciated replacement cost for an asset where the future economic benefits or service potential of the asset are not primarily dependent on the asset's ability to generate net cash inflows and where the Privacy Commissioner would, if deprived of the asset, replace its remaining future economic benefits or service potential.

If an asset's carrying amount exceeds its recoverable amount, the asset is impaired and the carrying amount is written down to the recoverable amount.

For assets not carried at a revalued amount, the total impairment loss is recognised in the statement of comprehensive income.

**Creditors and other payables**

Creditors and other payables are initially measured at fair value and subsequently measured at amortised cost using the effective interest method.

**Employee entitlements**

Employee entitlements that the Privacy Commissioner expects to be settled within 12 months of balance date are measured at undiscounted nominal values based on accrued entitlements at current rates of pay.

These include salaries and wages accrued up to balance date, annual leave earned, but not yet taken at balance date, retiring and long service leave entitlements expected to be settled within 12 months, and sick leave.

The Privacy Commissioner recognises a liability for sick leave to the extent that compensated absences in the coming year are expected to be greater than the sick leave entitlements earned in the coming year. The amount is calculated based on the unused sick leave entitlement that can be carried forward at balance date; to the extent the Privacy Commissioner anticipates it will be used by staff to cover those future absences.

The Privacy Commissioner recognises a liability and an expense for bonuses where it is contractually obliged to pay them, or where there is a past practice that has created a constructive obligation.

## **Superannuation schemes**

### **Defined contribution schemes**

Obligations for contributors to Kiwisaver and the National Provident Fund are accounted for as defined contribution superannuation scheme and are recognised as an expense in the statement of comprehensive income as incurred.

### **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 revenues and expenses in relation to financial instruments are recognised in the statement of comprehensive income.

### **Statement of cash flows**

Cash means cash balances on hand, held in bank accounts, demand deposits and other highly liquid investments in which the Privacy Commissioner invests as part of its day-to-day cash management.

Operating activities include all activities other than investing and financing activities. The cash inflows include all receipts from the sale of goods and services and other sources of revenue that support the Privacy Commissioner's operating activities. Cash outflows include payments made to employees, suppliers and for taxes.

Investing activities are those activities relating to the acquisition and disposal of current and non-current securities and any other non-current assets.

The Privacy Commissioner invests funds from time to time in short term investment accounts with the National Bank of New Zealand under standard terms and conditions.

The Privacy Commissioner receives income from Government Grant and some other income is received from Government Departments, the sale of publications and a programme of seminars and workshops undertaken.

### **Critical accounting estimates and assumptions**

In preparing these financial statements the Privacy Commissioner has made estimates and assumptions concerning the future. These estimates and assumptions may differ from the subsequent actual results. Estimates and assumptions are continually evaluated and are based on historical experience and other factors, including expectations of future events that are believed to be reasonable under the circumstances. The estimates and assumptions that have a significant risk of causing a material adjustment to the carrying amounts of assets and liabilities within the next financial year are discussed below:

**Property, plant and equipment useful lives and residual value**

At each balance date the Privacy Commissioner reviews the useful lives and residual values of its property, plant and equipment. Assessing the appropriateness of useful life and residual value estimates of property, plant and equipment requires the Privacy Commissioner to consider a number of factors such as the physical condition of the asset, expected period of use of the asset by the Privacy Commissioner, and expected disposal proceeds from the future sale of the asset.

An incorrect estimate of the useful life or residual value will impact the depreciation expense recognised in the statement of comprehensive income, and carrying amount of the asset in the statement of financial position.

The Privacy Commissioner minimises the risk of this estimation uncertainty by:

- physical inspection of assets;
- asset replacement programs;
- review of second hand market prices for similar assets; and
- analysis of prior asset sales.

The Privacy Commissioner has not made significant changes to past assumptions concerning useful lives and residual values. The carrying amounts of property, plant and equipment are disclosed in note 10.

**Critical judgements in applying the Privacy Commissioner's accounting policies**

Management has exercised the following critical judgements in applying the Privacy Commissioner's accounting policies for the period ended 30 June 2010:

**Leases classification**

Determining whether a lease agreement is a finance or an operating lease requires judgement as to whether the agreement transfers substantially all the risks and rewards of ownership to the Privacy Commissioner.

**Non-government grants**

The Privacy Commissioner must exercise judgement when recognising grant income to determine if conditions of the grant contract have been satisfied. This judgement will be based on the facts and circumstances that are evident for each grant contract.

### **Changes in accounting policies**

There have been no changes in accounting policies since the date of the last audited financial statements.

All policies have been applied on a basis consistent with previous years.

The Office has adopted the following revisions to accounting standards during the financial year which have had only a presentational or disclosure effect:

- NZ IAS 1 Presentation of Financial Statements (Revised 2007) replaces NZ IAS 1 *Presentation of Financial Statements (Issued 2004)*. The revised standard requires information in financial statements to be aggregated on the basis of shared characteristics and introduces a statement of comprehensive income. The statement of comprehensive income will enable readers to analyse changes in equity resulting from non-owner changes separately from transactions with owners. The Office has decided to prepare a single statement of comprehensive income for the year ended 30 June 2010 under the revised standard. Financial statement information for the year ended 30 June 2009 has been restated accordingly. Items of other comprehensive income presented in the statement of comprehensive income were previously recognised directly in the statement of changes in equity.
- Amendments to NZ IFRS 7 Financial Instruments: Disclosures. The amendments introduce a three-level fair value disclosure hierarchy that distinguishes fair value measurements by the significance of valuation inputs used. A maturity analysis of financial assets is also required to be prepared if this information is necessary to enable users of the financial statements to evaluate the nature and extent of liquidity risk. The transitional provisions of the amendment do not require disclosure of comparative information in the first year of application. The Office has elected to disclose comparative information.



## STATEMENT SPECIFYING COMPREHENSIVE INCOME

The Privacy Commissioner agreed the following financial targets with the Minister at the beginning of the year:

Specified comprehensive income	Target \$000	Achievement \$000
Operating Grant	3,148	3,148
Other Revenue	338	377
<b>Total Revenue</b>	<b>3,486</b>	<b>3,525</b>

### Output Operating Performance

The Privacy Commissioner committed to provide three output classes in 2009/10 to meet the requirements of the Minister of Justice in terms of their description, quantity, timeliness and costs.

Departmental Output Class Description	Target \$000	Achievement \$000
Privacy Policy	1,077	1,090
Information & 'Outreach'	915	925
Compliance	1,494	1,510
<b>Total</b>	<b>3,486</b>	<b>3,525</b>

## STATEMENT OF COMPREHENSIVE INCOME FOR THE YEAR ENDED 30 JUNE 2010

	Note	Actual 2010 \$000	Budget 2010 \$000	Actual 2009 \$000
Crown revenue	2	3,148	3,148	3,148
Other revenue/seminars	3	342	308	383
Interest income		35	30	69
<b>Total operating revenue</b>		<b>3,525</b>	<b>3,486</b>	<b>3,600</b>
Marketing	4	97	53	117
Audit Fees		21	18	21
Depreciation and Amortisation	1, 10, 11	171	150	202
Rental Expense		371	402	357
Operating Expenses		480	355	532
Staff Expenses	5	2,483	2,531	2,620
<b>Total Expenses</b>		<b>3,623</b>	<b>3,510</b>	<b>3,849</b>
<b>Total Comprehensive Income</b>		<b>(98)</b>	<b>(25)</b>	<b>(249)</b>

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

## STATEMENT OF MOVEMENTS IN EQUITY

### FOR THE YEAR ENDED 30 JUNE 2010

	Note	Actual 2010 \$000	Budget 2010 \$000	Actual 2009 \$000
Public equity as at 1 July		626	635	875
Total comprehensive income		(98)	(25)	(249)
<b>Total recognised revenues and expenses for the period</b>		<b>(98)</b>	<b>(25)</b>	<b>(249)</b>
Public equity as at 30 June	6	528	611	626

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

## STATEMENT OF FINANCIAL POSITION

### AS AT 30 JUNE 2010

	Note	Actual 2010 \$000	Budget 2010 \$000	Actual 2009 \$000
<b>PUBLIC EQUITY</b>				
General funds	6	528	611	626
<b>TOTAL PUBLIC EQUITY</b>		<b>528</b>	<b>611</b>	<b>626</b>
Represented by:				
<b>ASSETS</b>				
<b>Current assets</b>				
Cash and cash equivalents	7	465	705	620
Debtors and other Receivables	8	10	9	144
Prepayments	8	25	8	8
Inventory	9	10	4	10
<b>Total current assets</b>		<b>510</b>	<b>726</b>	<b>782</b>
<b>Non-current assets</b>				
Property, plant and equipment	10	292	210	280
Intangible assets	11	52	52	123
<b>Total non-current assets</b>		<b>344</b>	<b>262</b>	<b>403</b>
<b>Total assets</b>		<b>854</b>	<b>987</b>	<b>1,185</b>
<b>LIABILITIES</b>				
<b>Current liabilities</b>				
Creditors and other Payables	12	208	197	372
Employee entitlements	13	117	180	187
<b>Total current liabilities</b>		<b>325</b>	<b>377</b>	<b>559</b>
<b>Total liabilities</b>		<b>325</b>	<b>377</b>	<b>559</b>
<b>NET ASSETS</b>		<b>528</b>	<b>611</b>	<b>626</b>

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

## STATEMENT OF CASH FLOWS

### FOR THE YEAR ENDED 30 JUNE 2010

	Note	Actual 2010 \$000	Budget 2010 \$000	Actual 2009 \$000
<b>Cash Flows from operating activities</b>				
Cash was provided from:				
Supply of outputs to the Crown		3,384	3,148	3,148
Revenues from services provided		120	323	483
Interest received		35	30	69
Cash was applied to:				
Payments to suppliers		994	816	(952)
Payments to employees		2,570	2,578	(2,603)
Net Goods and Services Tax		19	(8)	(46)
<b>Net cash flows from operating activities</b>	<b>14</b>	<b>(42)</b>	<b>85</b>	<b>99</b>
<b>Cash Flows from Investing Activities</b>				
Cash was provided from:				
Cash was applied to:		-	-	-
Purchase of Property Plant and equipment		(113)	-	(13)
Purchase of Intangible Assets		-	-	-
<b>Net cash flows from investing activities</b>		<b>(113)</b>	<b>-</b>	<b>(13)</b>
Net increase (decrease) in cash held		(155)	85	86
Plus opening cash		620	620	534
<b>Closing cash balance</b>		<b>465</b>	<b>465</b>	<b>620</b>
Cash and bank		465	465	620
<b>Closing cash balance</b>		<b>465</b>	<b>465</b>	<b>620</b>

The GST (net) component of operating activities reflects the net GST paid and received with the Inland Revenue Department. The GST (net) component has been presented on a net basis, as the gross amounts do not provide meaningful information for financial statement purposes.

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

## STATEMENT OF COMMITMENTS

AS AT 30 JUNE 2010

	Actual 2010 \$000	Actual 2009 \$000
<b>Capital commitments approved and contracted</b>		
<b>Non-cancellable operating lease commitments, payable</b>		
Not later than one year	381	259
Later than one year and not later than two years	381	160
Later than two years and not later than five years	831	334
Later than five years	109	-

### Other non-cancellable contracts

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

The Privacy Commissioner leases two properties, one in Wellington and the other in Auckland. The lease on the property in Wellington expires December 2015. The property in Auckland has been sublet in part, due to it being surplus to current requirements. The lease on the Auckland premises expires 31 July 2013.

The Privacy Commissioner does not have the option to purchase the asset at the end of the lease term.

## STATEMENT OF CONTINGENT LIABILITIES

AS AT 30 JUNE 2010

Quantifiable contingent liabilities are as follows:

The Privacy Commissioner is subject to a "Make Good" clause in its lease contracts for the Auckland and Wellington offices. This clause, if invoked, would require the Privacy Commissioner to remove all leasehold improvements, and leave the premises in a state not dissimilar to that received at the time of moving into the premises. At balance date, the Privacy Commissioner's intention into the foreseeable future is to continue leasing the premises. The likelihood of this clause being invoked is unknown, as is the cost to fulfil the clause.

Other than that stated above, there are no known contingencies existing at balance date (2009 : nil).

## NOTES TO THE FINANCIAL STATEMENTS

### FOR THE YEAR ENDED 30 JUNE 2010

#### Note 1: Total Comprehensive Income

	Actual 2010 \$000	Actual 2009 \$000
The total comprehensive income is after charging for:		
Fees paid to auditors		
External audit		
Current Year	21	20
Prior Year	-	1
Depreciation:		
Furniture & Fittings	57	86
Computer Equipment	31	32
Office Equipment	12	19
<b>Total Depreciation for the year</b>	<b>100</b>	<b>137</b>
Amortisation of Intangibles	71	65
Rental expense on operating leases	371	356

#### Major budget variation

Explanations for significant variations from the Privacy Commissioner's budgeted figures in the statement of intent are as follows:

#### Statement of Comprehensive Income

##### *Other income/seminars*

The Office held a Privacy Forum during the year which provided additional other income on a cost recovery basis and offset by increased marketing expenditure.

##### *Operating expenses*

Operating expenses exceeded budget principally due to increased depreciation, computer maintenance and unbudgeted litigation. The additional expenditure in all areas was met from reserves held by the Privacy Commissioner. Contributing areas included:

##### *Marketing*

Expenditure associated with the Privacy Forum.

*Computer maintenance*

As hardware nears the end of its warranty periods we have been required to undertake additional maintenance to ensure business continuity.

*Litigation*

Prolonged litigation through to the Court of Appeal. The Privacy Commissioner was successful and though costs were awarded they were insufficient to fully meet actual costs.

*Depreciation*

Higher than budgeted depreciation due to changes associated with capital purchases and fitout of the Wellington office.

**Note 2: Public equity****Crown revenue**

The Privacy Commissioner has been provided with funding from the crown for specific purposes of the Privacy Commissioner as set out in its founding legislation and the scope of the relevant government appropriations. Apart from these general restrictions, there are no unfulfilled conditions or contingencies attached to government funding (2009 nil).

**Note 3: Other revenue**

	Actual 2010 \$000	Actual 2009 \$000
Other grants received	236	236
Rental income from property sub-leases	19	23
Privacy Forum	41	39
Seminars & Workshops	34	56
Sponsorship*	-	2
Other	12	27
<b>Total other revenue</b>	<b>342</b>	<b>383</b>

**Note 4: Marketing expenses**

	Actual 2010 \$000	Actual 2009 \$000
Website development expenses	19	33
Inventories consumed	26	19
Other marketing expenses	52	65
<b>Total marketing expenses</b>	<b>97</b>	<b>117</b>

**Note 5: Staff Expenses**

	Actual 2010 \$000	Actual 2009 \$000
Salaries and wages	2,279	2,410
Employer contributions to defined contribution plans	34	32
Other Staff expenses	126	28
Increase/(decrease) in employee entitlements (note 13)	(70)	17
Other contracted services	114	133
<b>Total Staff Expenses</b>	<b>2,483</b>	<b>2,620</b>

Employer contributions to defined contribution plans include contributions to Kiwisaver and the National Provident Fund.

**Note 6: General funds**

	Actual 2010 \$000	Actual 2009 \$000
Opening balance	626	875
Net (deficit) / surplus	(98)	(249)
<b>Closing balance</b>	<b>528</b>	<b>626</b>

**Note 7: Cash and cash equivalents**

	Actual 2010 \$000	Actual 2009 \$000
Cash on hand and at bank	47	270
Cash equivalents – term deposits	418	350
<b>Total cash and cash equivalents</b>	<b>465</b>	<b>620</b>

The carrying value of short-term deposits with maturity dates of three months or less approximates their fair value.

**Note 8: Receivables and prepayments**

	Actual 2010 \$000	Actual 2009 \$000
Trade debtors	10	144
Prepayments	25	8
<b>Total</b>	<b>35</b>	<b>152</b>

The carrying value of receivables approximates their fair value.

The carrying amount of receivables that would otherwise be past due, but not impaired, whose terms have been renegotiated is \$NIL (2009 \$NIL).

As at 30 June 2010 and 2009, all overdue receivables have been assessed for impairment. No debtors were past due. All receivables have been assessed for impairment and no debtors were impaired.

As at 30 June 2010 no debtors have been identified as insolvent. (2009 \$NIL).

**Note 9: Inventories**

	Actual 2010 \$000	Actual 2009 \$000
Publications held for sale	10	10

The carrying amount of inventories held for distribution that are measured at current replacement cost as at 30 June 2010 amounted to \$NIL (2009 \$NIL).

There have been no write-down of inventories held for distribution or reversals of write-downs (2009 \$NIL).



**Note 10: Property, plant and equipment**

Movements for each class of property, plant and equipment are as follows:

	Furniture and fittings \$000	Computer equipment \$000	Office equipment \$000	Total \$000
<b>Cost</b>				
Balance at 1 July 2008	481	146	114	741
Additions		13	-	13
Balance at 30 June 2009	481	159	114	754
Balance at 1 July 2009	481	159	114	754
Additions	80	32	2	114
Balance at 30 June 2010	561	191	116	868
<b>ACCUMULATED DEPRECIATION AND IMPAIRMENT LOSSES</b>				
Balance at 1 July 2008	191	71	75	337
Depreciation expense	86	33	19	138
Balance at 30 June 2009	277	104	94	475
Balance at 1 July 2009	277	104	94	475
Depreciation expense	57	31	12	100
Balance at 30 June 2010	334	134	107	575
<b>CARRYING AMOUNTS</b>				
At 1 July 2008				
At 30 June and 1 July 2009	204	55	20	279
At 30 June 2010	227	56	9	292

**Note 11: Intangible assets**

Movements for each class of intangible asset are as follows:

	Acquired software \$000
<b>COST</b>	
Balance at 1 July 2008	294
Additions	-
Balance at 30 June 2009	294
Balance at 1 July 2009	294
Additions	-
Balance at 30 June 2010	294
<b>ACCUMULATED AMORTISATION AND IMPAIRMENT LOSSES</b>	
Balance at 1 July 2008	106
Amortisation expense	65
Balance at 30 June 2009	171
Balance at 1 July 2009	171
Amortisation expense	71
Balance at 30 June 2010	242
<b>CARRYING AMOUNTS</b>	
At 1 July 2008	188
At 30 June and 1 July 2009	123
At 30 June 2010	52

There are no restrictions over the title of the Privacy Commissioner's intangible assets, nor are any intangible assets pledged as security for liabilities.

**Note 12: Creditors and other payables**

	Actual 2010 \$000	Actual 2009 \$000
Creditors	43	69
Income in advance	0	120
Accrued expenses	94	93
Other payables	71	90
<b>Total creditors and other payables</b>	<b>208</b>	<b>372</b>

Creditors and other payables are non-interest bearing and are normally settled on 30-day terms, therefore the carrying value of creditors and other payables approximates their fair value.

**Note 13: Employee entitlements**

	Actual 2010 \$000	Actual 2009 \$000
Current employee entitlements are represent by:		
Accrued salaries and wages	0	61
Annual leave	117	126
<b>Total current portion</b>	<b>117</b>	<b>187</b>
Current	117	187
Non-current	-	-

**Note 14: Reconciliation of total comprehensive income from operations with the net cashflows from operating activities**

	Actual 2010 \$000	Actual 2009 \$000
Total comprehensive income	(98)	(249)
Add (less) non-cash items:		
Depreciation and Amortisation	171	202
Other non Cash Items		-
<b>Total non-cash items</b>	<b>171</b>	<b>202</b>
Add (less) movements in working capital items:		
(Increase)/Decrease in receivables	134	(30)
(Increase)/Decrease in prepayments	(17)	-
(Increase)/Decrease in inventory	-	(6)
Increase/(Decrease)in payables	(44)	(15)
Increase/(Decrease)in employee entitlements	(70)	17
Increase/(Decrease) in Income in Advance	(120)	120
<b>Working capital movements - net</b>	<b>(119)</b>	<b>146</b>
Add (less) items classified as investing activities:		
Net loss (gain) on sale of assets	-	-
Total investing activity items	-	-
<b>Net cash flow from operating activities</b>	<b>(42)</b>	<b>99</b>

**Note 15: Related party information**

The Privacy Commissioner is a wholly owned entity of the Crown. The Government significantly influences the role of the Privacy Commissioner as well as being its major source of revenue.

The Privacy Commissioner is a Board Member of the Equal Employment Opportunities Trust. There were no transactions with this Trust during the current financial year. (In 2009 the Office paid the Trust \$200 for memberships fees.)

The Privacy Commissioner has entered into a number of transactions with government departments, Crown agencies and state-owned enterprises on an arm's length basis. Where those parties are acting in the course of their normal dealings with the Privacy

Commissioner, related party disclosures have not been made for transactions of this nature.

There were no other related party transactions.

#### Key management personnel compensation

	Actual 2010 \$000	Actual 2009 \$000
Total Salaries and other short-term employee benefits	832	832

Key management personnel include all Senior Management Team members, the Privacy Commissioner who together comprise the Leadership Team.

The Senior Management Team requested not to receive salary movements in the year ended 30 June 2010.

#### Note 16: Employees' Remuneration

The Office of the Privacy Commissioner, is a Crown Entity, and is required to disclose certain remuneration information in their annual reports. The information reported is the number of employees receiving total remuneration of \$100,000 or more per annum. In compliance, the table below has been produced, which is in \$10,000 bands to preserve the privacy of individuals.

Total remuneration and benefits	Number of Employees	
	Actual 2010 \$000	Actual 2009 \$000
\$100,000 - \$110,000	1	
\$110,000 - \$120,000		
\$120,000 - \$130,000	1	1
\$130,000 - \$140,000	1	1
\$140,000 - \$150,000	1	1
\$150,000 - \$160,000		
\$160,000 - \$170,000	1	1

**Note 17: Commissioners' Total Remuneration**

In accordance with the disclosure requirements of Section 152 (1)(a) of the Crown Entities Act 2004, the total remuneration includes all benefits paid during the period 1 July 2009 to 30 June 2010.

Name	Position	Amount 2010	Amount 2009
Marie Shroff	Privacy Commissioner	\$263,502	\$263,502

**Note 18: Cessation Payments**

No redundancy payments were made in the year. (2009 : NIL)

**Note 19: Indemnity Insurance**

The Privacy Commissioner's insurance policy covers public liability of \$3 million and professional indemnity insurance of \$250,000.

**Note 20: Post Balance Date Events**

There are no adjusting events after balance date of such importance that non-disclosure would affect the ability of the users of the financial report to make proper evaluations and decisions.

**Note 21: Financial instruments****Note 21A: Financial instrument categories**

The accounting policies for financial instruments have been applied to the line items below:

	2010 \$000	2009 \$000
<b>FINANCIAL ASSETS</b>		
<b>Loans and Receivables</b>		
Cash and cash equivalents	465	620
Debtors and other receivables	10	144
Total loans and receivables	475	764
<b>FINANCIAL LIABILITIES</b>		
<b>Financial liabilities at amortised cost</b>		
Creditors and other payables	208	372
Total financial liabilities at amortised cost	208	372

**Note 21B: Financial instruments risk**

The Privacy Commissioner has a series of policies providing risk management for interest rates, operating and capital expenditures denominated in a foreign currency, and the concentration of credit. The Privacy Commissioner is risk averse and seeks to minimise its exposure from its treasury activities. Its policies do not allow any transactions which are speculative in nature to be entered into.

**Credit risk**

Credit risk is the risk that a third party will default on its obligation to the Privacy Commissioner, causing the Privacy Commissioner to incur a loss. Financial instruments which potentially subject the Office to risk consist principally of cash, short term investments, and trade receivables.

The Privacy Commissioner has a minimal credit risk in its holdings of various financial instruments. These instruments include cash, bank deposits.

The Privacy Commissioner places its investments with institutions that have a high credit rating. The Privacy Commissioner believes that these policies reduce the risk of any loss which could arise from its investment activities. The Privacy Commissioner does not require any collateral or security to support financial instruments.

There is no significant concentration of credit risk.

The maximum amount of credit risk for each class is the carrying amount in the Statement of Financial Position.

**Fair value**

The fair value of other financial instruments is equivalent to the carrying amount disclosed in the Statement of Financial Position.

**Currency risk**

Currency risk is the risk that the value of a financial instrument will fluctuate due to changes in foreign exchange rates.

The Privacy Commissioner has no exposure to currency risk.

**Interest rate risk**

Interest rate risk is the risk that the value of a financial instrument will fluctuate due to changes in market interest rates. There are no interest rate options or interest rate swap options in place as at 30 June 2010 (2009: NIL). The Privacy Commissioner has no exposure to interest rate risk.

**Liquidity risk**

Liquidity risk is the risk that the Privacy Commissioner will encounter difficulty raising

liquid funds to meet commitments as they fall due. Prudent liquidity risk management implies maintaining sufficient cash, the availability of funding through an adequate amount of committed credit facilities and the ability to close out market positions. The Privacy Commissioner aims to maintain flexibility in funding by keeping committed credit lines available.

In meeting its liquidity requirements, the Privacy Commissioner maintains a target level of investments that must mature within specified timeframes.

### Market risk

#### *Fair value interest rate risk*

The Privacy Commissioner's exposure to fair value interest rate risk is limited to its bank deposits which are held at fixed rates of interest. The Privacy Commissioner does not hold significant interest-bearing assets, and have no interest-bearing liabilities. The Privacy Commissioner invests cash and cash equivalents with the National Bank, ensuring a fair market return on any cash position, but do not seek to speculate on interest returns, and do not specifically monitor exposure to interest rate returns.

#### Cash flow interest rate risk

Cash flow interest rate risk is the risk that the cash flows from term deposits held at the National Bank will fluctuate because of changes in market interest rates. The Privacy Commissioner does not consider that there is any significant interest exposure on the Privacy Commissioner's investments. The Privacy Commissioner is primarily exposed to changes in the New Zealand Dollar Official Cash Rate.

#### Interest rate exposure – maturity profile of financial instruments

The following tables are based on the earlier contractual re-pricing or maturity period.

	Weighted average effective interest rate %	Variable interest rate NZ\$000	Fixed maturity dates – less than 1 year NZ\$000	Non interest bearing NZ\$000
<b>2010</b>				
<b>Financial assets</b>				
Cash and cash equivalents	3	465	-	-
	<b>3</b>	<b>465</b>	<b>-</b>	<b>-</b>
<b>2009</b>				
<b>Financial Assets</b>				
Cash and cash equivalents	5.88	620	-	-
	<b>5.88</b>	<b>620</b>	<b>-</b>	<b>-</b>



### Interest rate sensitivity

The sensitivity (percentage movement) analysis in the table below of the effect on net surplus has been determined based on the exposure to interest rates at the reporting date and the stipulated change taking place at the beginning of the financial year and held constant throughout the reporting period. A 100 basis point change is used when reporting interest rate risk internally to the Commissioner and represents Privacy Commissioner's assessment of a reasonably possible change in interest rates.

	Net surplus 2010 NZ\$000	Net surplus 2009 NZ\$000
Cash and cash equivalents +100 bps	4.65	6.2
Cash and cash equivalents – 100 bps	(4.65)	(6.2)

Privacy's sensitivity to interest rate changes has not changed significantly from the prior year.





