

Privacy Commissioner  
Annual Report 2009

# Privacy Commissioner

Annual Report 2009



Privacy Commissioner  
Te Mana Matapono Matatapu



Privacy Commissioner  
Te Mana Matapono Matatapu

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

© 2009 The Privacy Commissioner

ISSN 0 478 11729 9

# Annual Report of the Privacy Commissioner

For the year ended 30 June 2009

Presented to the House of Representatives

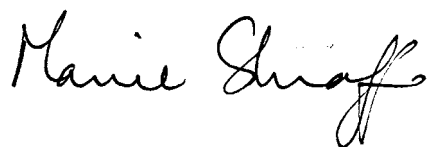
Pursuant to section 24 of the Privacy Act 1993



November 2009

**THE MINISTER OF JUSTICE**

I tender my report as Privacy Commissioner for the year ended 30 June 2009

A handwritten signature in black ink, reading "Marie Shroff". The signature is written in a cursive, flowing style with a prominent loop at the end of the last name.

Marie Shroff

Privacy Commissioner

## CONTENTS

1: KEY POINTS .....	5
2: INTRODUCTION .....	9
3: OFFICE AND FUNCTIONS OF THE PRIVACY COMMISSIONER .....	17
Independence and competing interests .....	17
Complaints .....	17
Education and publicity .....	17
Legislation and policy .....	17
Information matching programmes .....	18
Codes of practice .....	18
Reporting .....	18
Equal employment opportunities .....	18
Staff .....	19
4. REPORT ON ACTIVITIES .....	21
International activities .....	21
Highlights .....	21
Information services .....	22
Enquiries .....	22
Training and education .....	23
Privacy Awareness Week .....	23
Website .....	24
Other outreach .....	24
Media .....	24
Complaints and access reviews .....	24
Complaints received .....	25
Complaints closed .....	26
Age of complaints .....	27
Complaint outcomes .....	28
Settled complaints .....	29
Personal contact and settlement .....	29
Top respondent agencies .....	30
Agency types .....	32
Human Rights Review Tribunal .....	32
Commissioner initiated inquiries .....	33
Medical notes and insurers .....	33
Section 54 authorisations .....	34
Policy .....	34
Health policy .....	35
Technology policy .....	35
Law Commission's review of privacy .....	35

## CONTENTS

Information matching .....	36
Legislation .....	36
Codes of practice .....	37
Functions under other enactments .....	37
Complaints and reviews .....	37
Oversight of information disclosure arrangements .....	37
Consultations on complaints handled by other agencies .....	37
Consultations with the Ombudsmen .....	38
5. INFORMATION MATCHING .....	41
Information matching and privacy – an introduction .....	41
Glossary .....	42
The year in information matching .....	42
Electoral Enrolment Centre match activity .....	43
Ministry of Health information handling .....	43
Data security project .....	44
Outreach .....	44
Changes in authorised and operating programmes .....	44
Online transfer approvals .....	45
OPC reporting .....	47
Programme Reports .....	47
1. Corrections/ACC Prisoners Programme .....	47
2. IR/ACC Levies and Compensation Programme .....	48
3. Citizenship/BDM Citizenship by Birth Processing Programme .....	48
4. BDM/DIA(C) Citizenship Application Processing Programme .....	49
5. BDM/DIA(P) Passport Eligibility Programme .....	50
6. Citizenship/DIA(P) Passport Eligibility Programme .....	50
7. NZTA/EEC Unenrolled Voters Programme .....	51
8. MoT/EEC Unenrolled Voters Programme .....	52
9. MSD/EEC Unenrolled Voters Programme .....	52
10. Citizenship/EEC Unenrolled Voters Programme .....	53
11. INZ/EEC Unqualified Voters Programme .....	54
12. BDM (Deaths)/GSF Eligibility Programme .....	54
13. BDM (Deaths)/INZ Deceased Temporary Visa Holders Programme .....	55
14. Citizenship/INZ Entitlement to Reside Programme .....	55
15. Corrections/INZ Prisoners Programme .....	56
16. Customs/IR Child Support Alerts Programme .....	57
17. Customs/IR Student Loan Interest Programme .....	57
18. MSD/IR Working For Families Tax Credits Administration Programme .....	58
19. MSD/IR Working for Families Tax Credits Double Payment Programme .....	58

## CONTENTS

20. Customs/Justice Fines Defaulters Alerts Programme .....	59
21. INZ/Justice Fines Defaulters Tracing Programme .....	60
22. IR/Justice Fines Defaulters Tracing Programme.....	61
23. MSD/Justice Fines Defaulters Tracing Programme .....	62
24. Customs/MED Motor Vehicle Traders Importers Programme .....	62
25. MoT/MED Motor Vehicle Traders Sellers Programme .....	63
26. BDM (Births)/Ministry of Health NHI and Mortality Register Programme.....	64
27. BDM (Deaths)/Ministry of Health NHI and Mortality Register Programme .....	65
28. ACC/MSD Benefit Eligibility Programme .....	66
29. BDM/MSD Identity Verification Programme .....	66
30. BDM (Deaths)/MSD Deceased Persons Programme .....	67
31. BDM (Marriages)/MSD Married Persons Programme .....	68
32. Centrelink/MSD Change in Circumstances Programme .....	69
33. Centrelink/MSD Periods of Residence Programme .....	69
34. Corrections/MSD Prisoners Programme.....	70
35. Customs/MSD Arrivals and Departures Programme .....	71
36. Customs/MSD Periods of Residence Programme.....	71
37. Educational Institutions/MSD (StudyLink) Loans and Allowances Programme .....	72
38. Employers/MSD Section 11A Social Security Act Programme .....	73
39. HNZ/MSD Benefit Eligibility Programme .....	73
40. IR/MSD Commencement/Cessation Benefits Programme .....	74
41. IRD/MSD Commencement/Cessation Students Programme .....	75
42. IR/MSD Community Services Card Programme .....	76
43. IR/MSD Debtors Tracing Programme .....	77
44. IR/MSD (Netherlands) Tax Information Programme .....	77
45. Ministry of Education/MSD (StudyLink) Results of Study Programme.....	78
46. Netherlands/MSD Change in Circumstances Programme .....	78
47. Netherlands/MSD Debt Recovery Programme .....	79
48. Netherlands/MSD General Adjustment Programme .....	79
49. BDM (Deaths)/NPF Eligibility Programme .....	79
50. BDM (Deaths)/NZTA Deceased Driver Licence Holders Programme .....	80
6. FINANCIAL AND PERFORMANCE STATEMENTS .....	82
Statement of responsibility .....	83
Audit report .....	84
Statement of objectives and service performance 2008/09 .....	86
Statement of accounting policies .....	97
Statement specifying financial performance .....	104
Statement of financial performance .....	105
Statement of changes in equity .....	105



## CONTENTS

Statement of financial position .....	106
Statement of cash flows .....	107
Statement of commitments .....	108
Statement of contingent liabilities .....	108
Notes to the financial statements .....	109
<b>Section 3 Tables</b>	
Table 1: Office of the Privacy Commissioner workplace gender profile 2008/09 .....	19
Table 2: Office of the Privacy Commissioner workplace ethnic profile 2008/09 .....	19
<b>Section 4 Tables</b>	
Table 3: Complaints received and closed 2004–2009 .....	25
Table 4: Act/code – breakdown of complaints received 2008/09 (previous year in brackets) ...	25
Table 5: Principles/rules in complaints received 2008/09.....	26
Table 6: Act/code – breakdown of complaints closed 2008/09 (previous year in brackets) ...	26
Table 7: Principles/rules in closed complaints 2008/09 .....	27
Table 8: Age of complaints closed 2008/09 (previous year in brackets).....	28
Table 9: Outcomes on closed files 2008/09 .....	29
Table 10: Complaints received and closed for top respondent agencies 2008/09 .....	31
Table 11: Outcomes for top respondent agencies 2008/09.....	31
Table 12: Agency type 2008/09 (previous year in brackets).....	32
Table 13: Referrals, tribunal cases and outcomes 2003–2009 .....	33
<b>Section 5 tables</b>	
Table 14: Short term online approvals 2008/09.....	46
Table 15: Longer term online approvals 2008/09 .....	46
<b>Figures</b>	
Figure 1: Total files and files over 12 months old .....	27
Figure 2: Age of complaints in progress as at 30 June 2009 .....	28
Figure 3: Active authorised information matching programmes 2008/09 .....	43
Figure 4: Authorised and active information matching programmes .....	45



# 1: KEY POINTS

## Information and communications

- Our nationwide public opinion survey showed that concern about personal information and privacy issues has grown or remained high, especially in relation to the internet and business.
- We received 6,632 enquiries from members of the public and organisations seeking our advice on personal information and privacy matters. This was more than 1,200 up on 2007/08.
- There has been a large growth in media interest with 216 media enquiries received. Our average number of media enquiries in recent years was around 150 per year.
- We published “Privacy at Work” to provide straightforward guidance on privacy issues for employers and employees.
- Our survey on use of portable storage devices by government agencies identified a need for many agencies to improve their practices.
- We held two Privacy Awareness Weeks during this reporting year, working with our partners from the Asia Pacific Privacy Authorities (APPA) forum, and with strong support from business and government agencies in New Zealand.
- The Office delivered 60 privacy education workshops and seminars to members of the public and stakeholder groups as well as over 40 presentations by the Commissioner and staff to wide range of audiences (such as Chambers of Commerce, health or business groups).

## Investigations

- 806 privacy complaints were received, up from 662 in the previous year.
- 24 percent of complaints were closed by settlement or mediation, which is a large increase.
- 95 percent of complaints are under 12 months of age, with 83 percent closed within six months of receipt.

## Policy and technology

- There are now 50 active government information matching programmes that we monitor, 27 of which use online data transfers.
- Policy work during the 2008/09 year involved a wide range of projects with central and local government, the private sector, industry bodies and voluntary organisations. Significant areas include border control issues, employee browsing, and research and consultation on information sharing in government.
- Health information privacy continues to raise significant issues, for instance electronic health records, newborn metabolic screening and expansion of the DNA database used for criminal investigations.
- The Law Commission’s major review of privacy continued. By the end of the reporting period the Commission was beginning the review of the Privacy Act itself. Final reports are expected during 2010.
- The major review of the Credit Reporting Privacy Code involving industry and other stakeholders has commenced and will continue through 2009/10. Current Australian reforms in the area will be taken into account.
- We released the findings of an “own initiative” inquiry into the practices of medical insurance companies in seeking full medical records.

## International

- The OECD adopted its Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy, which the Office helped to develop.
- The Privacy (Cross-border Information) Amendment Bill will eliminate barriers to cross-border enforcement cooperation. It should enable New Zealand to obtain a finding from the European Union that our law is 'adequate', providing legal authority for European agencies to freely send data to New Zealand for processing.
- At our initiative, the International Conference of Data Protection and Privacy Commissioners established a process to seek observer status before APEC, the OECD, Council of Europe and the International Organization for Standardization (ISO) ensuring privacy input into international policy and standards development.





## 2: INTRODUCTION

Recessionary economic pressures have been pre-occupying most sectors of the economy in the past year. Demand for many products and services has taken a dive. Businesses are re-grouping to cope with the huge challenges they are facing. They are re-evaluating essential priorities and shaping future directions. This may involve re-thinking the way businesses collect, store and use personal data. Practices that were adequate to carry a business through the boom times may not stack up when competition for the next customer is fierce. A recent KPMG survey showed that eight out of 10 organisations were looking to IT-based solutions as a way to cut costs and manage through the difficult economy.<sup>1</sup> Good customer data handling can be designed in, and become a competitive advantage for businesses.

The public sector is affected differently by the recession – there may be no shortage of customers, but there are redundancies, budget cuts and the expectation to do more with less. Like business, the public sector needs to equip itself for surviving not only the gloom of today, but for brighter days in coming months. I question whether public sector leaders are grasping that opportunity to lift their ICT practices – certainly when it comes to the way citizens' data is handled. Recent events and reactions have given cause for real doubt – such as the data breaches reported to us. The power of information technology is one of the big stories of the 21st century. It poses an enormous risk – and any responsible public sector manager should be doing a risk analysis on how information is handled in their agency and making sure there are protections in place.

Technological functionality carries some inherent business risks. If the organisational culture is silent when it comes to information security and protection of personal information, some employees will fill in the gaps – not necessarily correctly – and with consequent reputational and business damage. We have responded proactively by trying to assess the level of risk that public sector agencies, in particular, may face. Our survey on the use of portable storage devices (PSDs) was one example; another was the study of data encryption in government data matching programmes.

### PSD survey results – personal information at risk

The PSD survey was the first of its kind undertaken in New Zealand to find out what precautions government agencies are taking to secure New Zealanders' data.

PSDs include USB sticks, cell phones, BlackBerries, iPhones, iPods, MP3 players, PDAs (personal digital assistants) and netbooks. They are used for a variety of purposes, including: to take work home or information to meetings; as temporary file storage or backup; or to transfer sometimes sensitive bulk data between organisations. They are small, lightweight and can store vast amounts of information. PSDs are easy to use and easy to lose. Surveying PSD use provides an indicative snapshot of how agencies are protecting data.

We were particularly concerned about the use of personal PSDs in the workplace. It is so easy to mislay one, or to accidentally disclose sensitive information by, for example, lending a USB stick to a friend. People using personal PSDs for work are also more likely to accidentally take that corporate information with them when they change jobs.

Our survey of the 42 main government agencies showed PSDs were widely used but that there were real gaps in security procedures and practices.

1. KPMG, Technology Industry Executive Survey Points to Economic Recovery: A Survey of Industry Executives, August 2009.

Thirty-five out of the 37 agencies that responded to the survey (95 percent) made PSDs available to staff – most commonly USB sticks. Nearly two-thirds of agencies also allowed staff to use personal PSDs for work purposes.

Just nine of the agencies made PSD encryption mandatory, while 43 percent did not provide encryption solutions of any sort. Sixty-two percent kept a PSD register but only 22 percent said they would be able to track transfers of data to PSDs.

Although the survey found 75 percent of the government agencies had policies to restrict or control the use of PSDs, we are not yet confident that those policies are of a good standard, followed in practice or are well known by staff.

- Only half of the policies included details about how to delete content.
- Only 25 percent of agencies performed an audit to ensure PSD procedures were followed.
- Seventy percent had procedures to report the loss or theft of a corporate PSD, but only 27 percent for personal PSDs used for work.
- Availability and use of security tools – such as encryption, tracking of data transfers, or hardware and software controls – was patchy or lacking.

Agencies that held the most sensitive classified information had significantly tighter controls over the use of PSDs than those that held the largest amounts of personal information.

It was particularly concerning that some of the agencies with poorer practices were flagship departments that hold the personal details of millions of New Zealanders. I am forced to the conclusion that personal information about New Zealanders is not being treated with the same care and respect as other sorts of ‘classified’ or ‘sensitive’ information.

There have been many overseas incidents that demonstrate how easily PSDs containing large amounts of sensitive information are lost or mislaid, including:

- November 2008, loss of the unencrypted details about almost 900 customers – including accounts, phone numbers and addresses – by a Bank of Ireland employee.
- December 2008, loss of a USB stick containing details about more than 6,000 United Kingdom prisoners.
- A UK survey, carried out by a data security firm, found an estimated 9,000 USB sticks were left in people’s pockets when they took their clothes to the dry cleaners.

To prevent similar events affecting New Zealanders, we need to “get it right before we get it wrong”.

After our PSD survey, we provided tips to organisations on the safe use of PSDs including:

- having a formal policy on PSD use;
- making staff aware of the need and procedures to report the loss or theft of a PSD;
- using encryption for all PSDs that are likely to store personal information; and
- monitoring and auditing the use of PSDs; enforcing strict limits on the use of personal PSDs.

### **Data encryption in the public sector**

In early 2008, we carried out a review of the way files used in government information matching programmes were being transferred.



At the time, my staff found that while all tapes, CDs and floppy disks were transferred within New Zealand by means that we considered to be reasonably secure – typically delivered by staff by hand or, where a courier was used, involving a ‘track and trace’ facility – there was a failure to encrypt that data.

Of those files that were not encrypted, some were password protected, but others did not even have that level of protection. Of 46 information matching programmes, we found data for 19 was being transferred physically on unencrypted digital media.

I made my expectation clear then that files being transferred for use in these government programmes – often involving thousands of individual records – should be encrypted.

Some departments indicated they were already in negotiations to move to more secure methods and I was encouraged by the serious attention to security displayed by all departments participating in data matching.

However, we pointed out then that transfers for the purposes of authorised information matching were merely one stream of intra-governmental data transfers. I called on those involved in security practices in other areas as well to carefully reflect on the need for encryption for all portable data storage media. Those comments still do not appear to have been heeded by some of the core departments.

I strongly urge middle and senior public sector managers to become more focused on data protection. This is a huge area – and it does not appear that government agencies have grasped that. This is the information century; data and its protection are part of our critical infrastructure. Generally New Zealanders trust the public sector to handle their information well. That trust can easily be lost. Our survey showed public unease about government personal data sharing has grown sharply. People should start seeing information handling as part of a business risk analysis – in just the same way they have policies and practices about health and safety, they need policies and practices about information handling. These are not new messages for the public sector.

Government agencies need to recognise that the information they hold about people is also one of their major assets, and one they must protect as carefully as they would a physical asset. While some government leaders are making a significant effort to do this, overall the public sector is slow in becoming aware that their information databases are assets that have to be protected.

I might be inspired to have more confidence if I were not also hearing repeatedly of instances where things have gone wrong. Government agencies are losing data – sometimes in hardcopy and sometimes in digital form. It concerns me when I am not advised of these incidents at the time, but instead discover them through alternative channels. It also concerns me when the departments involved fail to see the signals that their practices need sharpening up. In today’s climate, departments can and must do better.

## Growth in demand

The Office is facing increasing external demand across its areas of work. Complaint numbers have risen significantly in the past year – more than 800 complaints were received during the 2008/09 year, which is an increase on the average of around 650 for each of the past four years. Similarly, the number of enquiries received from members of the public and businesses seeking our advice on privacy matters has grown to over 6,600. This is about 1,200 more public enquiries than in 2007/08 and is the highest number of enquiries received since 2002.

## Media and privacy

The number of enquiries from media has almost doubled in the past year to 216. Numbers alone are just part of the picture; the range and nature of the enquiries has also shifted.

Many media enquiries were related to developments in information or communication technology. Subjects that generated multiple enquiries included: Google products and platforms such as Street View; the increase and sophistication of closed-circuit television (CCTV); social networking, particularly Facebook; developments in the use of DNA-based science; genetic privacy, including the Guthrie blood-spot cards; and data security issues, including various data breaches.

The evidently multi-national character to personal data collection forms the background landscape. The person in Whangarei or Waimate is engaging with international giants when they upload their Facebook page or store their health records online. New Zealand children travelling through the United States relinquish their biometric information for permanent retention and exchange under the US Patriot Act. New Zealanders applying online for a job may find their CV and application is stored in a US-based server. Companies are increasingly storing and processing personal records remotely, 'in the cloud'. New Zealand laws and regulation will be of limited help in such instances, and whatever protections can be arrived at need to have an international dimension.

One consequence of the shifting nature of media calls towards the wider, technology based, threats to privacy is that we deal with fewer enquiries where some restrictive notion of 'privacy' is put forward as a block to common sense. Journalists, like the rest of us, are increasingly technologically savvy. Moreover, there is wider recognition that personal information has been commodified and can be treated in the same way as any other asset; it may be traded, sold or even stolen. Protection of personal information is a modern necessity. This development is particularly apparent online, where new industries are springing up to cater for the burgeoning market in personal data.

In a report for the Broadcasting Standards Authority, journalist Colin Peacock points out that the media and the public tend to hold different views of privacy.<sup>2</sup>

***Journalists aren't necessarily unsympathetic about 'maintaining standards consistent with the privacy of the individual' as the standard says, but their instinct is obviously to reveal as much as possible about any given story. There is also a gulf between the media's attitudes to privacy and those of the public ...***

***A survey in 2005<sup>3</sup> found that many people think broadcasters should always explain to people participating in broadcasts precisely how their contributions will be used on air, and when. More than half those surveyed said people should be given an advance screening of the part in which they feature. These expectations are clearly unrealistic – even unfeasible – as far as the media are concerned.***

2. Colin Peacock, Principles and Pragmatism: An Assessment of Broadcasting Standards Authority Decisions from a Journalist's Perspective / Nga Matapono Me Te Mahi Whai Kiko: He Arotakenga I Nga Whakataua a Te Mana Whanonga Kaipaho, Ki Ta Te Kaikawe Korero Titiro (Broadcasting Standards Authority, 2009).

3. Real Media Real People – Privacy and information consent in broadcasting, Broadcasting Standards Authority, 2004.

The news media of course has dual functions – acting both as a channel for information to the wider community and as a voice for public concerns. A shift in approach by the media is significant on at least those two fronts. Not only does it mean that the public is being offered, and is digesting, a more balanced diet – it perhaps also reflects changing public preoccupations and attitudes.

## Public attitudes – UMR survey results

Public opinion surveys act as useful gauges for the Office, both to tell us what the public is concerned about and to measure changing attitudes. They also help us determine our strategic direction and priorities for future work.

The results of the most recent survey were released in August 2008.<sup>4</sup> The survey showed that many New Zealanders have a strong and growing awareness of privacy and information technology issues. For example, almost a third (32 percent) of people surveyed in 2008 reported that they had become more concerned about issues of individual privacy and personal information in the past few years.

The results from the survey for business were clear: there were very high levels of concern about potential breaches of individual privacy by business. Ninety percent of people said they would be concerned (including 74 percent ‘very concerned’) if a business they did not know got hold of their personal information. Eighty-six percent were concerned if information supplied to a business for one purpose was used for another purpose.

Trust is a signal element – for business and for government. We asked people about the level of trust they had in the way different organisations protected or used personal information. Results varied widely. Health service providers, including doctors, hospitals and pharmacies rated highly, with 92 percent of respondents saying they were trustworthy. Trust in Police handling of personal information was also high (84 percent). Approximately two-thirds of respondents said they trusted the way government departments (65 percent) and ACC (69 percent) handled personal information. Businesses selling over the internet recorded the lowest levels of trust (25 percent) for their personal information handling.

These trust indicators are particularly important for government because so much of what government does depends on public acceptance and cooperation. Government cannot afford to spoil public trust in its processes through avoidable events. Overseas, data losses across the UK public service led the British Prime Minister to announce a review of data handling in government in November 2007.<sup>5</sup> The report noted the challenges:

***... [T]he public have a right to expect the information that they provide to Government will be held securely and used appropriately. The Government’s ability to deliver and improve public services relies on high levels of public trust. Government has always regarded personal data of citizens as a critical asset akin to the most sensitive financial and other information handled within Departments. This should continue to be Government’s underlying principle. The challenge is to ensure that information is collected, used, and, where appropriate, shared, effectively and securely.***

4. UMR Research surveys - see [www.privacy.org.nz](http://www.privacy.org.nz). The previous survey was commissioned in 2006.

5. UK Cabinet Office, Data Handling Procedures in Government: Interim Progress Report, December 2007. The final report was released in June 2008. Both are available at [www.cabinetoffice.gov.uk](http://www.cabinetoffice.gov.uk)

New Zealand government agencies face equivalent challenges. We asked people how they felt about government departments sharing personal information. Concern rose from 37 percent to 62 percent between the 2006 and 2008 surveys. Perhaps this was partly due to making the question clearer – but it certainly shows underlying unease.

The results also underline the need for caution by government in assuming public knowledge of key technology infrastructure or systems. For instance, we asked respondents if they were aware that everyone in New Zealand has their own national health index number, which identifies them in the health system. Half of respondents (50 percent) were unaware.

We are in the middle of an information revolution. Technology enables details about individuals to be collected, used and disclosed on an unprecedented scale, both in New Zealand and overseas. These survey results give clear messages to both business and government about the need to protect information in order to retain customer trust.

### Law Commission's review of privacy

I noted last year that the Law Commission's review of New Zealand privacy laws had begun. It is a very extensive and thorough project with four main parts. Part 1, a policy overview, has been completed and a study paper issued. Part 2 was devoted to public registers and a report with recommendations has been released, but will not be implemented until a comprehensive review of the Privacy Act 1993 has been completed. Part 3 looked at the adequacy of New Zealand's civil and criminal law to deal with invasions of privacy, and an issues paper was published in March 2009 and submissions were received. The final report for Part 3 is expected near the end of 2009.

As of June 2009, the Law Commission had begun its review of the Privacy Act, which represents Part 4 of the review. This will be a particularly compelling stage of the review process because the Commission is now in the midst of exploring new options, both for this Office and for the Act. The Commission has been working hard to get to grips with privacy and all its permutations. It has consulted widely and considered the very modern challenges to data protection, especially arising from technology and science.

There is still quite a lot of ground to cover before the Law Commission puts forward its final report and recommendations to the Government. While we expect many of the Privacy Act's fundamental features, based on international norms, will remain, there is much wiggle-room and opportunity for improvement.

The review is an opportunity to equip the Office with tools for the future. There may be a role for new approaches, whether by auditing government and business processes, or through the ability to enforce decisions. There have been many changes to the legal landscape since the Office was established in the early 1990s – not the least of which is the growth in complaint agencies – and we are very willing to look at new ways to resolve privacy disputes. It has become apparent over time that the nature of the complaints the Office receives reflects only a certain portion of privacy-related incidents. Of course some people will choose not to complain but, more importantly, many of the very concerning and systemic issues do not come to light by way of a complaint. The media highlights some of those concerns, while others come to our attention through the policy work we are engaged in. Different types of problems require a different tool set and the Law Commission's review will help to ensure we have kitted ourselves out to deal with those new challenges.

## Tools for the future

New Zealand business is operating in a global data processing economy and our data protection law needs to be recognised as stacking up internationally. Our privacy law must keep pace so that New Zealand businesses can take advantage of opportunities in the digital age. Beyond that broad aim, there are a variety of mechanisms that would help ensure that the sort of data protection New Zealanders can expect is up to speed with the demands of a modern information-driven society.

One of those tools would be a finding from the European Union that New Zealand's Privacy Act provides an "adequate" level of protection for any European personal data that might be transferred to, or through, New Zealand. This might on the face of it sound pretty obscure – and in some ways that is correct – but it should have a practical effect and help to open up trading opportunities with Europe. The largely technical changes that are necessary to our law to help achieve this were introduced to Parliament in April 2009, through the Privacy (Cross-border Information) Amendment Bill. This sort of development is especially important in the current global economic climate.

The Bill will have two main impacts: first, it will help ensure New Zealand law meets the expectations of our trading partners, and second, it will remove an anomaly so that people living overseas can access their personal information held in New Zealand. The Bill will also give the Privacy Commissioner the ability to cooperate with overseas privacy authorities when dealing with, or transferring, privacy complaints. This reflects a priority area in the privacy work of both the Asia-Pacific Economic Cooperation (APEC) forum and the Organisation for Economic Co-operation and Development (OECD).

These measures are important and necessary steps to update the Privacy Act, protect our international trading position and improve access to personal information. We have been waiting for this change for a long time. I expect this Bill to be the first part of a more extensive modernisation of the Privacy Act. It is complementary to the thorough privacy review currently being carried out by the Law Commission.



# 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. This means 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 an interference 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 Privacy Commissioner's 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. Increasingly, enquirers go to the website for information.

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

Part of the Commissioner's role is to make public statements on matters affecting privacy, and the Office maintains open communication with the news media. 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 have some impact on the privacy of the individual or classes of individuals. Many such 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; and
- reporting to the Prime Minister on any matter that should be drawn to his or her attention and, 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; and
- 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.

### **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 2008/09 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; and
- making family-friendly practices available to all staff (for example, flexible working hours).  
Expected benefits include lower staff turnover, stress reduction for employees, better recruitment possibilities, a greater range of diversity in staff interests and experience, and greater overall flexibility in deploying staff.

The Commissioner continues to place a strong emphasis on fostering a diverse workplace and inclusive culture.



**TABLE 1:** OFFICE OF THE PRIVACY COMMISSIONER WORKPLACE GENDER PROFILE 2008/09

	Women		Men		Total
	Full-time	Part-time	Full-time	Part-time	
Commissioner	1				1
Senior Managers	2		3		5
Team Leaders	3				3
Investigating Officers	3		2		5
Administrative Support	6	1	1		8
Advisors (Technology & Policy)	2		4		6
Enquiries Officers	1		1		2
<b>Total</b>	<b>18</b>	<b>1</b>	<b>11</b>		<b>30</b>

**TABLE 2:** OFFICE OF THE PRIVACY COMMISSIONER WORKPLACE ETHNIC PROFILE 2008/09

	Māori		Pacific Peoples		Asian (incl. 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									5	
Team Leaders									3	
Investigating Officers									5	
Administrative Support							1		6	1
Advisors (Technology & Policy)									6	
Enquiries Officers									2	

## Staff

Staff are employed by the Privacy Commissioner in the Auckland and Wellington offices.

The Assistant Commissioner (Policy) has responsibility for work on codes of practice, legislation, data matching and policy matters, and privacy issues associated with technology. The Assistant Commissioner (Legal) is the Commissioner’s legal counsel and has responsibility for litigation, communications, education and enquiries functions, and contributes to complaints work. The Assistant Commissioner (Investigations) has responsibility for complaints and investigations functions and manages teams of investigating officers in both offices. In addition, 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, legal, enquiries, writing, accounting and publication work for the Office.

At their own request, in recognition of the seriousness of the economic situation, the Commissioner, Assistant Commissioners and General Manager have received no remuneration increase in calendar year 2009. The majority of other staff in the Office did not receive a salary increase.



# 4. REPORT ON ACTIVITIES

## International activities

In the growing world of e-commerce and cross-border trade, such as offshore data processing, New Zealand needs to meet the privacy standards of trading partners to better facilitate and protect our trading relationships.

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

This year, a particular priority has been enhancing or, in some cases, creating mechanisms to promote cooperation amongst overseas privacy enforcement authorities and regulators.

### Highlights

#### *Privacy (Cross-border Information) Amendment Bill*

Following adoption by the OECD of its Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy, which the Office helped develop, we assisted New Zealand government agencies develop a mechanism for inclusion in the Privacy (Cross-border Information) Amendment Bill to facilitate referral of complaints to overseas privacy enforcement authorities. The amendments will help eliminate barriers to cross-border enforcement cooperation.

The Bill will amend the Privacy Act to provide the Commissioner with powers to intervene where certain cross-border transfers warrant action. This should enable New Zealand obtain a finding from the European Union that our law provides an 'adequate standard of data protection'. Such a finding would provide European organisations with legal authority to freely send data to New Zealand for processing. The removal of some existing impediments to business information flows from Europe could provide a competitive advantage for New Zealand businesses.

#### *International Conference of Data Protection and Privacy Commissioners*

At our initiative, the International Conference of Data Protection and Privacy Commissioners established a process to observe and contribute to the meetings of relevant international organisations active in privacy standard setting. This involved establishing a steering group, led by New Zealand, to initially seek observer status before APEC, the OECD, Council of Europe and the International Organization for Standardization (ISO). These international organisations have standing committees devoted to information privacy issues, and the initiative will enable the collective input of Privacy Commissioners from around the world to be better harnessed to achieve global results.

#### *International secondments*

We continue to foster collaboration between data protection authorities and promote best practice in the field of privacy regulation. Secondments were identified as a particularly useful tool to enhance staff skills and development, and provide opportunities for the transfer of knowledge between information privacy specialists in the Asia-Pacific region.

Over the past two years, the Office has assisted the Asia Pacific Privacy Authorities Forum (APPA) develop a framework for secondments. During the year, an Australian Privacy Commissioner's Office staff member spent a successful two-month secondment with our technology team.

#### *APEC Privacy Pathfinder*

The Office continued to contribute to the APEC Privacy Pathfinder, which seeks to progress the international implementation of the APEC Privacy Framework. The Office's focus has been on sub-projects devoted to developing an arrangement for cross-border cooperation amongst privacy enforcement authorities.

#### *Memorandum of Understanding with the Australian Privacy Commissioner*

The Office's Memorandum of Understanding (MOU) with the Australian Privacy Commissioner was reviewed and a new MOU put in place. One particularly successful initiative has been establishing occasional teleconferences between senior management in both offices.

#### *Interdepartmental group*

Given the variety of ways in which international developments can affect privacy policy making and cross-border personal information flows, the Office has convened an informal interdepartmental group on international privacy issues for the past several years. These meetings typically bring the Office together with officials from the Ministry of Economic Development, State Services Commission, Ministry of Justice, Ministry of Foreign Affairs and Trade and, during the current review of privacy law in New Zealand, the Law Commission. The group meets as required, usually two or three times a year.

#### *Forums*

In addition to these highlights, the Office continues to engage in international activities in a variety of ways. The forums the Office principally contributes to include:

- APPA – meets twice a year and involves commissioners from Australia, Canada, Hong Kong, Korea and New Zealand;
- International Conference of Data Protection and Privacy Commissioners – 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 Data Privacy Subgroup – this specialist group is part of APEC's efforts to provide a safe environment for electronic commerce; and
- OECD Working Party on Information Security and Privacy (WPISP) – brings together privacy expertise across OECD countries to advance policy objectives.

## **Information services**

### **Enquiries**

During the 2008/09 year, we received 6,632 enquiries from members of the public and organisations seeking our advice on privacy matters – more than 1,200 up on 2007/08 and the highest number since 2002. The subjects callers enquired about were as widely varied as ever. It is therefore hard to pinpoint the reason for the sharp rise. We will continue to monitor the situation, but at this stage it appears enquiries are the result of increased public awareness about privacy issues following the many media stories, from both New Zealand and overseas.

Topics that stood out as attracting enquiries included:

- Release of information about Trade Me members to a prisoner as part of the criminal proceedings discovery process. We initiated an inquiry into the event, the result of which is pending.
- Letters sent by New Zealand First to electors at the time of the election, indicating that a website had been set up in the elector's name. In fact, the site was simply a way of delivering information

about New Zealand First directly to that elector, and was not searchable on the internet. However, it was apparent that many people misunderstood the process and believed New Zealand First had put their name on the internet. This caused concern and in some cases considerable distress.

- The launch of Google Street View in New Zealand. Most enquirers expressed concern, but some were in favour of the new application.

Other topics of interest during the year included the use of personal details for direct marketing, storage and access to medical files when the medical practitioner has retired or died, and employment issues such as covert recording in the workplace. Businesses often required advice on issues such as writing privacy statements for their websites. We also received a range of calls from schools, or their advisers, about topics such as rights of non-custodial parents to access information about their child and confidentiality of information held by school counsellors.

### Training and education

This was a busy year for the Office's education work. There were 60 privacy workshops and seminars, most conducted by the investigations staff, with some provided by contractors. Health continued to be a popular subject for education, but many agencies, both in the public and the private sector, have been able to take advantage of our workshops on the operation of the Privacy Act. Seminars and workshops were held in Auckland, Hamilton, New Plymouth, Palmerston North, Wellington, Nelson and Christchurch.

### Privacy Awareness Week

We ran two Privacy Awareness Weeks during this reporting year, working with our partners in the APPA forum. The reason for having two weeks was that our standard date of August coincided unhelpfully with the summer vacation in Canada and British Columbia, which have recently joined APPA. The first week in May suited all the APPA jurisdictions.

The highlights of the August 2008 Week were:

- a one-day Privacy Issues Forum in Wellington, with over 200 attendees;
- the inaugural exhibition of Chris Slane's cartoons;
- a business breakfast in Auckland, in partnership with the Chamber of Commerce;
- publication of our booklet "Privacy at work", with straightforward guidance on privacy issues for employers and employees; and
- publication of our public opinion survey on privacy, run by UMR Research.

We also built on existing partnerships with external organisations, including the Computer Society and privacy officer groups, and established new relationships with organisations such as Information Systems and Control Association (ISACA).

While the May 2009 Week was relatively low-key (predominantly because of staff availability) the partnership aspect grew considerably. Many organisations decided to coordinate their activities with Privacy Awareness Week, or otherwise support it, for instance with media statements about privacy issues. These organisations included Trade Me, Unisys, the Police, Ministry of Justice, Marketing Association and Netsafe.

Other highlights included:

- the Chris Slane cartoon exhibition in Auckland;
- the launch in Christchurch of the results of our survey on use of portable storage devices;
- two technology and privacy forums (in Wellington and Auckland); and
- two security breach workshops in Wellington.

Privacy Awareness Week is now well established in New Zealand, Australia, Hong Kong, Korea and Canada. The European privacy jurisdictions also run a data protection day in January. Building on the success of these regional events, the International Conference of Data Protection and Privacy Commissioners is currently considering whether to organise a global privacy day or week.

### Website

Our website continues to be a major source of information for the public, businesses and other organisations in New Zealand and overseas. We have further enhanced the site this year by adding two particular features.

The first is easily accessible information about how we, the Human Rights Review Tribunal and the Courts interpret the privacy principles. We launched the first stage of the project – which deals with explaining rights of access to and correction of personal information – during Privacy Awareness Week in May 2009. The information is set out in easily navigable layers, so that visitors can choose what level of detail they need – from a straightforward explanation through to examples of how the principles apply in real life, and on to the text of a relevant Tribunal or court case. The website gives us the ideal tool to do this.

The second feature is an interactive, password-protected forum for privacy officers. This is a space in which they can seek advice from us or from their fellow privacy officers, where they can share existing policies or ‘workshop’ new ones, and receive information about upcoming events such as meetings of privacy officer organisations.

### Other outreach

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

- privacy in the information century;
- user-centred government;
- why good privacy is good business;
- privacy myths and realities;
- privacy by design;
- managing disclosures in the context of mental health;
- privacy in the employment context; and
- online communication and social networking.

### Media

The Office is facing considerable growth in demand in media enquiries. During the 2008/09 year, we received 216 enquiries from print, radio and other media about news stories and events with a privacy or data protection angle. This number is a clear increase on the average number of 150 media enquiries in recent years. Topics were varied, but many related to developments in information or communication technology. Subjects that particularly generated enquiries were Google products, such as Street View; the increase and sophistication of closed-circuit television (CCTV); social networking, particularly Facebook; developments in the use of DNA-based science; genetic privacy, including the Guthrie blood-spot cards; and data security issues, including various data breaches.

### Complaints and access reviews

A total of 806 complaints was received in the 2008/09 year. This is a significant increase compared with totals for each of the previous four years. Table 3 shows incoming and closed complaints and work in progress at year-end.

An analysis shows that all areas of complaints have increased. No particular reason is evident, but we suspect that a general rise in awareness of privacy issues may be a key factor. Recessionary pressures do not appear to be directly influencing complaints, although we suspect that difficult economic times are playing some part.

Within the past few years, the investigations team has been engaged in a process to improve efficiency and quality of outcome on each and every complaint. Those efforts are reflected in the work in progress at year-end. At the end of 2008/09 year, 273 complaints remained open. This represents a steady improvement in the age of complaints open and the time taken to complete complaints. The current work in progress total is within usual expectations of between 250 to 350 files.

**TABLE 3:** COMPLAINTS RECEIVED AND CLOSED 2004-2009

	2004/05	2005/06	2006/07	2007/08	2008/09
Complaints received	721	636	640	662	806
Complaints closed	970	752	701	767	822
Work in progress after year-end	571	455	394	289	273

### Complaints received

Of the 806 complaints received, the vast majority alleged breaches or interference with privacy under the information privacy principles within the Act. Table 4 shows a breakdown between complaints under the privacy principles and rules in the three main codes operating under the Act. These figures represent the general actions investigated on each file, recognising that many complaints involve several principles.

**TABLE 4:** ACT/CODE – BREAKDOWN OF COMPLAINTS RECEIVED 2008/09 (previous year in brackets)

Act/Code	Number
Privacy Act	659 (538)
Health Information Privacy Code	139 (100)
Telecommunications Privacy Code	1(10)
Credit Reporting Code	7(14)
<b>Total</b>	<b>806 (662)</b>

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 categories involving access to, correction of and retention of personal information made up 56 percent of the investigative workload in complaint numbers. Our experience is that access complaints are particularly time consuming to assess and work through. Investigations into use and disclosure were the next largest group with slightly more than 20 percent of complaints involving those types of actions. Complaints about collection actions were 13 percent of our work.

**TABLE 5:** PRINCIPLES/RULES IN COMPLAINTS RECEIVED 2008/09

Principle or rule	Number
Purpose for collection	33
Source of information	38
Collection of information	30
Manner of collection	26
Storage of information	73
Access to information	461
Correction of information	57
Accuracy of information	30
Retention of information	11
Use of information	17
Disclosure of information	192
Unique identifier use	2
Charging	10
<b>Total</b>	<b>980</b>

Total is higher than number of complaints because some complaints involve more than one principle or rule.

### Complaints closed

Of the 822 complaint files closed during the year, the majority were matters raised under the privacy principles (see Table 6). The three Codes accounted for 18 percent of the closed files.

**TABLE 6:** ACT/CODE – BREAKDOWN ON COMPLAINTS CLOSED 2008/09 (previous year in brackets)

Act/Code	Number
Information Privacy Principle	673 (632)
Health Information Privacy Code	133 (117)
Telecommunications Privacy Code	6 (5)
Credit Reporting Code	10 (13)
<b>Total</b>	<b>822 (767)</b>

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



**TABLE 7:** PRINCIPLES/RULES IN CLOSED COMPLAINTS 2008/09

Principle or rule	Number
Purpose for collection	28
Source of information	49
Collection of information	33
Manner of collection	27
Storage of information	100
Access to information	462
Correction of information	69
Accuracy of information	23
Retention of information	7
Use of information	24
Disclosure of information	206
Charging	3
<b>TOTAL</b>	<b>1031</b>

### Age of complaints

At the end of the year, 14 complaints (5 percent of work in progress) were files older than 12 months. The majority of those files were within 18 months old. Those older than 18 months were files delayed by litigation or extensive legal argument. Figure 1 shows a month-by-month breakdown of work in progress at the end of each month and the number of files more than 12 months old.

*Figure 1: Total files and files over 12 months old*

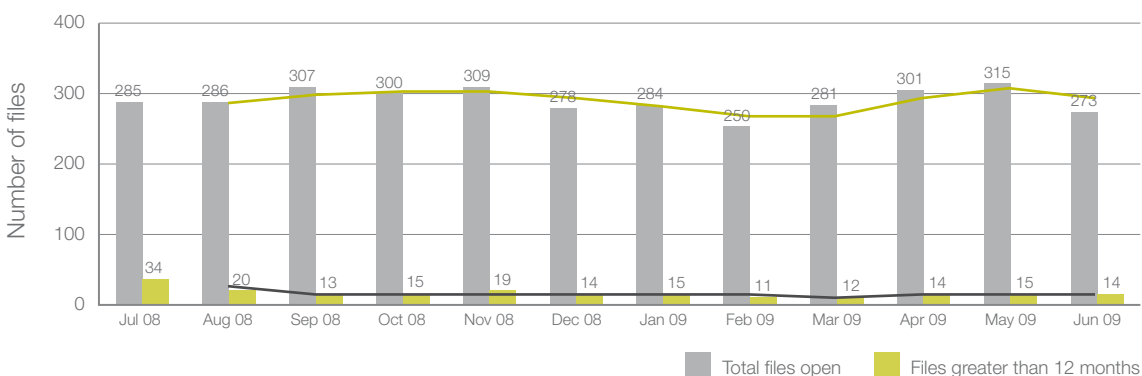


Table 8 shows the age of complaints closed in 2008/09 (previous year in brackets). During the 2007/08 year, 84 percent of closed complaints were closed within the year. For 2008/09, that figure has improved to 94 percent. Significantly, the number of complaints that were dealt with inside six months increased from 61 percent to 74 percent of complaints closed.

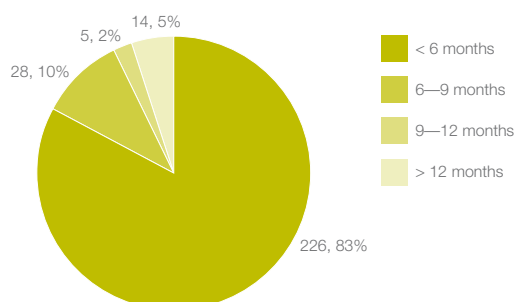
**TABLE 8:** AGE OF COMPLAINTS CLOSED 2008/09 (previous year in brackets)

Age of complaint	Number closed	Percentage closed*
6 months or less	608 (465)	74% (61%)
6 months to 9 months	103 (113)	13% (15%)
9 months to 1 year	59 ( 62)	7% (8%)
> 1 year	52 (127)	6% (16%)
<b>Total</b>	<b>822 (767)</b>	<b>(100%)</b>

\* Numbers have been rounded in the percentage column

Figure 2 shows the age range of complaints that remained as work in progress at the end of the year. At the end of the 2007/08 year, 88 percent of work in progress was under 12 months of age. At the end of the 2008/09, 95 percent was under 12 months and a significant 83 percent was under six months of age. Our continuing aim is to complete 90 percent of complaints within nine months of receipt.

*Figure 2: Age of complaints in progress as at 30 June 2009*



### Complaint outcomes

In preceding years, the investigations team was divided into two, with one team dealing with the early assessment and conciliation of incoming complaints, and the other dealing with complaints that required greater effort and work to resolve.

This year, we trialled a one-team approach by consolidating assessment and conciliation and further investigative processes. This meant that investigating officers undertook both work-streams at the same time and that a complaint generally had only one investigator during its lifetime. In addition, the resources of the office were used in a more generalist way allowing the investigations team to be more responsive to increased work-flows and to times where capacity was depleted or challenged. In addition, all of the investigations team was able to advance early settlement, rather than half as under the previous model. The trial has been successful and enabled the team to improve efficiency and effectiveness.

Table 9 shows the variety of outcomes in complaints closed during 2008/09. The figures do not correlate with the number of complaints closed, as any one particular complaint may have a variety of allegations and outcomes. For example, a complaint may involve the Office providing an opinion that an interference of privacy has been demonstrated on the facts, which then prompts a settlement by the parties. In addition, a complaint may involve several alleged breaches of principles or rules and the outcome might be different for each principle or rule. For example, an agency may be found not

to have breached its obligations under principle 6 to provide access to information, but as a consequence of the investigation, it may become apparent that the agency has breached its obligations under the Act to ensure that information is stored appropriately.

**TABLE 9:** OUTCOMES ON CLOSED FILES 2008/09

Further investigation inappropriate	Withdrawn by complainant	Complainant failed to pursue complaint	Settled/mediated	No interference decision	Interference decision	Referred to Director of Proceedings
91	57	74	193	431	104	12

All of the outcome figures represent complaints, except for the interference/no interference and settlement numbers, which may cover multiple allegations on single files.

A total of 91 files were closed because it was inappropriate to continue investigations. In many cases these closures were the result of investigations showing there was a more appropriate and adequate remedy than could be achieved by completing the complaint process or that the actions complained about did not demonstrate any discernable privacy issue.

In 2007/08, 20 complaints were referred to the Director of Human Rights Proceedings; for 2008/09, 12 were referred. Significantly, this total has reduced while settlements have risen. We suspect that agencies are actively seeking to avoid a referral to the Director of Human Rights Proceedings and the potential for time-consuming litigation.

**Settled complaints**

Of the complaints closed, 193 were settled or mediated. This is a 43 percent increase on settlement compared with the previous year and represents 24 percent of the files closed for the year.

The new investigations team structure and style has enabled a greater focus on settlement as an outcome for complainants and respondents. As in previous years, settlement outcomes were variable according to the expectations and willingness of parties to reach consensus. Many access to personal information complaints were settled because the respondent agency accepted the views of the Commissioner and released information previously withheld. Often an assurance that a practice would be stopped or changed, and demonstrated within agency policy or guidelines, was sufficient for some complainants. A genuine apology may satisfy many complainants. In addition, a number of complaints involved monetary compensation. Most monetary compensation was for amounts less than \$5,000 but with some closer to \$20,000.

**Personal contact and settlement**

The investigations team continued to improve efficiency, as displayed within the timeliness statistics mentioned earlier. In addition, the team also sought to improve effectiveness and quality on all complaints by ensuring an outcome that met the expectations of all parties.

Our goal is to increase the rate of settlement and the personal contact with the parties to a complaint. The preferred method is at least to communicate with parties by phone or, if possible, face-to-face, recognising that written communications alone will not ensure people feel they are heard and understood. We aim to have a conversation with as many of our complainants and respondents as possible. During the 2008/09 year, 80 percent of complaint files involved a member of the investigations team talking with one or both of the parties, usually by phone. We aim to improve that percentage in the future.

We also believe that conversations and direct early contact will increase the potential for settlement outcomes. In 2008/09, our settlement outcomes increased in number and many complaints were settled much earlier than previously anticipated.

#### *Satisfaction survey*

The effectiveness of our complaint processes was also measured by a satisfaction survey. For the six months January to June 2009, every complainant and respondent received a satisfaction survey form with the closing letter, along with a prepaid envelope. The survey is completed anonymously.

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

For respondent agencies subject to multiple complaints, a single survey was sent near the end of the 2008/09 year. Ninety-two surveys were returned, with 70 percent of those from complainants. The questions asked the participant to rate the various factors on a scale of one to five, with the lower numbers representing negative comment and the higher numbers positive comment. A score of three would represent satisfied. Of the returned surveys the results were:

- 80 percent said they were satisfied or very satisfied with the service;
- 93 percent had expectations of a good to very good service;
- 77 percent felt their expectations were met or bettered;
- 83 percent agreed or strongly agreed that staff were competent;
- 90 percent agreed or strongly agreed that staff kept their promises;
- 80 percent agreed or strongly agreed that they were treated fairly;
- 71 percent agreed or strongly agreed that their individual circumstances were considered; and
- 77 percent agreed or strongly agreed that the service was good value for taxpayer money.

The survey has shown that most people who use our service find it satisfactory. However, the results also indicate areas that we could look to improve. We will continue to survey all complainants and respondents who engage with our complaints process.

#### **Top respondent agencies**

During the 2008/09 year, seven agencies made double figures in complaints received by the Commissioner. Two of the agencies, the Ministry of Justice and New Zealand Security Intelligence Service, were newcomers to the list. During the previous year, the only non-governmental agency to make the list was Veda Advantage, a credit-reporting agency. It did not make the 2008/09 list.

**TABLE 10:** COMPLAINTS RECEIVED AND CLOSED FOR TOP RESPONDENT AGENCIES 2008/09

Agency	Number of complaints received	Number of complaints closed
New Zealand Police	76	62
Ministry of Social Development	62	57
Department of Corrections	44	44
Accident Compensation Corporation	43	39
Department of Labour (Immigration)	42	70
Ministry of Justice	11	13
NZ Security Intelligence Service	11	9
<b>Total</b>	<b>289</b>	<b>294</b>

Table 10 sets out the complaints received and the number closed throughout the 2008/09 year. In total, these agencies constituted more than a third of the Commissioner’s complaints handling work, as was the case the previous year.

**TABLE 11:** OUTCOMES FOR TOP RESPONDENT AGENCIES 2008/09

Agency	Further investigation inappropriate (no case)	Withdrawn by complainant	Complainant failed to pursue	Settled/mediated	No interference	Interference	Referred to Director of Proceedings
Police	2	5	5	8	63	16	4
Ministry of Social Development	3	9	8	8	45	5	0
Department of Corrections	4	3	5	9	33	1	0
Accident Compensation Corporation	4	1	2	4	32	5	0
Department of Labour (Immigration)	0	5	2	13	67	33	1
Ministry of Justice	3	1	2	6	5	0	0
NZ Security Intelligence Service	0	1	0	0	0	0	0

Table 11 shows the various outcomes on complaints closed for each respondent. As in Table 9, all the figures represent complaint files except those for interference/no interference and settlement, which cover multiple allegations on single files.

The single agency complained about most was the Police, and naturally the higher outcomes follow. There is also a notable increase in settlement outcomes for all agencies as demonstrated in the outcomes.

The New Zealand Security Intelligence Service featured on the reported list for the first time. The Service has had an unprecedented demand for access to personal information prompted by several high-profile news media cases where information was released about well-known New Zealanders.

The Department of Labour (Immigration) had a high rate of interference with privacy findings driven largely by incomplete information releases on various complaints. Many of those were minor and technical in nature, and referral to the Director of Proceedings was not warranted in such circumstances. Only one of the complaints was referred to the Director, while many were resolved or settled by a release of information.

### Agency types

Table 12 provides a break down of complaints in various sectors. The numbers of complaints in the reported sectors are very similar to those in previous years. All areas have increased largely commensurate with the general increase in complaints for the year.

The public sector accounted for 56 percent of the Commissioner’s complaints work in 2008/09, which was a repeat of trends in earlier years.

**TABLE 12:** AGENCY TYPE 2008/09 (previous year in brackets)

Agency type	Total	Percentage
Government sector, including education and local authorities	371 (293)	46 (44)
Health sector, including hospitals and medical practices	121 (100)	15 (15)
Financial sector, including banking, insurance, credit agencies and debt collectors	91 (81)	11 (12)
Other	223 (188)	28 (29)
<b>Total</b>	<b>806</b>	<b>(100)</b>

### Human Rights Review Tribunal

The Human Rights Review Tribunal (HRRT) is the specialist Tribunal that 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 12 cases to the Director of Human Rights Proceedings (DHRP) in 2008/09, where we found that an interference with privacy had occurred and the parties were unable to settle their dispute. The Director is a completely independent officer. If we refer a matter to him, he decides whether to take plaintiff proceedings against the agency. The Director filed four claims in the Tribunal during the course of the 2008/09 year, to add to three claims that were filed before the start of the year but had not yet proceeded to a substantive hearing, and two claims in which the Tribunal issued substantive decisions. In addition, the Director settled eight complaints that we had referred to him (some settlements involving compensation for the complainant). He declined to take proceedings in two complaints that we referred because it became apparent that there would be evidential difficulties.

A complainant can also take proceedings directly in the Tribunal. Most complainant-initiated proceedings result from situations where we have found that there is no interference with privacy. This year, 25 complainants filed new cases in the Tribunal, to add to the Director’s four. As the table shows, this represents an unusually high number of new proceedings. At the time of publication, most of these proceedings were still at a preliminary stage.

The Tribunal issued 10 interlocutory decisions on such questions as jurisdiction, name suppression or strike-out applications. Three strike-out applications were successful. It also issued seven ‘substantive’ decisions, only one of which resulted in a finding of interference with privacy, and four costs decisions.

In addition there were four appeals to the High Court, one of which was successful in relation to a small matter but for the most part was unsuccessful, and the remaining three were wholly unsuccessful.

**TABLE 13:** REFERRALS, TRIBUNAL CASES AND OUTCOMES 2003-2009

	2003/04	2004/05	2005/06	2006/07	2007/08	2008/09
Referrals to DHRP	0	13	12	15	20	12
New proceedings	19	9	17	22	19	29
Settled/ withdrawn (in HRRT)	6	4	6	4	6	3
Costs decisions*	–	–	–	5	5	4
Struck out	7	2	16	2	19	3
No interference	7	2	5	4	4	6
Interference found	2	3	5	3	0	1

\*Costs decisions only recorded since 2006/07

## Commissioner initiated inquiries

### Medical notes and insurers

During the 2008/09 year, the Privacy Commissioner concluded her inquiry into the practice by insurance companies of collecting full medical notes for a specified number of years. The inquiry concluded that insurers that collected full medical notes – even for a specified period – were at risk of breaching the Health Information Privacy Code. This is because insurers can only collect personal health information that is necessary to make insurance decisions, such as calculating whether to insure someone or whether to pay out on a claim.

Insurers do need to collect detailed medical information to make insurance decisions, and their clients need to be completely open and honest about that information. However, this should usually take the form of asking for answers to particular questions. Not all the information contained in medical notes is necessarily relevant to an insurance decision. For instance, medical notes may contain family or relationship information – the medical practitioner may have treated a person as a whole, in their individual circumstances and context. This will not always be relevant to the decisions the insurer has to make about cover or claims.

Occasionally, an insurer will be entitled to collect full medical notes if the more specific information does not provide the detail the insurer needs to make the decision. However, these situations should be rare.

The inquiry also concluded that insurers needed to take care to ensure their clients clearly authorised the insurer to collect their health information from their medical practitioner. In particular, the insurance client should be asked to provide a separate authorisation for collection of full medical notes. Also, for the authorisation to be reasonably “informed”, the insurer should tell the client why full medical notes are required in these circumstances.

The inquiry has been well received by the medical profession and by most insurers. However, some insurers have indicated that they may continue to collect full notes as they did before. This may well result in complaints being made to us.

## 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. The power to grant specific exemptions gives the Act extra flexibility by taking account of unanticipated collection, use or disclosure of information that is in the public interest, or in the interests of the person concerned. Section 54 can be useful when some disclosure ought to be made in the public interest but there is a duty under the Act not to disclose and the agency has not yet formulated a clear policy enabling disclosure. It can also act as a ‘safety valve’ to address rare and unexpected problems.

In considering applications under section 54, the Commissioner must first be satisfied that the proposed action would in fact breach principle 2, 10 or 11. Many applications fail on this first point.

The Commissioner then evaluates whether, in the special circumstances of the case, any interference with the privacy of the individual that could result is substantially outweighed by either the:

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

A guidance note to assist any agency considering applying for an authorisation is available on the Privacy Commissioner’s website or by contacting the Office.

One application was received during the 2008/09 year, but no authorisation was granted.

## 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 throughout the entire process.

Policy work during the 2008/09 year included a wide range of projects with central and local government, the private sector, industry bodies and voluntary organisations. Continuing the 2007/08 trend, 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 also undertaken some policy projects, such as developing guidance material for agencies. This has included work on employee browsing and on information sharing between public sector agencies. The latter is a major on-going project requiring consultation with agencies to uncover what, if any, barriers they face to sharing information with other agencies. Guidance material for agencies explaining how the Privacy Act can be applied to information sharing activities should be available within the next few months.



Another significant area of work has focused on 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 assist agencies identify any potential impacts on individuals' privacy and mitigate these while still responding to the challenges they face.

### 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 contributing to a review of the Newborn Metabolic Screening Programme ('Guthrie Cards'), development of a health information consumer forum in conjunction with the Health Information Strategy Advisory Committee, responding to the Health and Disability Commissioner's review of his Act, and the development of a position on the proposal to expand the use of DNA samples under the Criminal Investigations (Bodily Samples) Amendment Bill.

### Technology policy

Major topics that have arisen this year are similar to those in 2007/08. These include biometrics, video surveillance, portable storage devices, smartcards, ISO standards relating to information technology security and privacy, web-based computing services and on-line identity authentication systems.

To support this work, we seek to raise awareness of privacy as it relates to specific technologies through our on-going 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 six forums during 2008/09 were held in Wellington and Auckland to audiences of up to 100 people. They covered topics such as web-based computing services, ICT security, sensor-based environments and differing international perspectives on technology and privacy.

We also initiate our own technology and privacy research projects within the Office. This year, we surveyed 42 central government agencies about their use of 'portable storage devices' (PSDs). PSDs are small, lightweight, portable, easy to use devices capable of storing and transferring large volumes of information, and can be easily lost, misplaced, forgotten or stolen. Using them in the workplace presents potential security risks, particularly if the devices contain unsecured or sensitive data. The survey results show PSDs are widely used by government, but there are real gaps in procedure and practice. For example, at the time of the survey, 75 percent of agencies had procedures in place to report the loss or theft of a PSD, but 44 percent did not have procedures for disposing of obsolete PSDs, and only 25 percent of agencies performed an audit to ensure PSD use procedures were followed.

The full results of the survey were released during Privacy Awareness Week 2009, and were followed by the Privacy Commissioner issuing guidelines to help government agencies, businesses and other organisations manage the privacy risks associated with PSD use. We will run a follow-up survey in the 2009/10 year.

### Law Commission's review of privacy

The Law Commission has completed the first two stages of its four-stage Review of Privacy and by the end of the reporting period was working on stages 3 and 4.

The Stage 1 study paper, Privacy Concepts and Issues, was a high level policy overview that established a conceptual framework, examined social attitudes, changes in technology and international trends relating to privacy. It does not include recommendations.

The second report, Public Registers: Review of the Law of Privacy Stage 2, recommends a review of all public registers by a dedicated team. The recommendations are currently on hold and will be considered by the Government when the full Privacy Act review is completed.

Stage 3 deals with the adequacy of New Zealand's civil and criminal law to deal with invasions of privacy. In particular, the Commission looked at the tort of invasion of privacy and whether any additional regulation is needed for surveillance that occurs outside of law enforcement agencies. An Issues Paper was released calling for comment on the options identified. We made a detailed submission on the stage 3 paper, including on areas such as the tort, surveillance and civil and criminal remedies, and released an associated media statement.

The Commission has now embarked upon stage 4 – a review of the Privacy Act 1993. We are closely engaged with stage 4 and developing proposals for reforming the Privacy Act, including those from our 1998 review of the Act (Necessary & Desirable). We welcome and support the Law Commission's view that the Act is fundamentally sound, but that it requires some amendment to better address the challenges of modern information and communications technology. We also support the Commission's consideration of whether the Office requires enforcement powers to deal efficiently and effectively with unlawful practices, especially systemic ones related to expanding uses of technology. An issues paper is expected at the end of 2009.

The reports are available at [www.lawcom.govt.nz](http://www.lawcom.govt.nz).

## 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 50 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. Significant work went into the final drafting stages of the Anti Money Laundering and Financing of Terrorism Bill to ensure that changes to the collection of personal information, and subsequent use and disclosure, were as privacy protective as possible.

We also devoted considerable resources to the final stages of the Immigration Bill (and associated supplementary order papers). The Immigration Bill essentially reworks the immigration system to bring it into line with current technologies and practices. Part of this involves the collection and use of biometric information by government agencies, which is relatively new in New Zealand (notwithstanding the long use of fingerprints), and there are clear and strong privacy interests involved. Our input has helped the Immigration Bill to be drafted in a manner that better balances the privacy and public interests.

We have also commented extensively on a suite of bills from the Ministry of Justice (Collections) designed to enhance the collection of outstanding fines and reparation owed to the Courts. This has included the Vehicle Confiscation and Seizure Bill and the Summary Proceedings Amendment Bill.

## Codes of practice

Work on codes of practice during the 2008/09 year has included:

- approval and issuing of an amendment to the Justice Sector Unique Identifier Code (Amendment No 2);
- ongoing review of the Credit Reporting Privacy Code; and
- revocation of the Post-Compulsory Education Unique Identifier Code.

## 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. Parliament has sometimes required 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. Examples of these functions follow.

### Complaints and reviews

- Health Act 1956 (s.22F) – concerning refusals to transfer medical records between providers;
- Domestic Violence Act 1995 (ss.118-120) – reviews of decisions to refuse suppression directions for entries on public registers; and
- Social Security Act 1964 (s.11B) – complaints of breaches of the Ministry of Social Development’s code of conduct governing its use of powers to demand information.

### Oversight of information disclosure arrangements

- Passports Act 1992 (s.36) – requires the Secretary for Internal Affairs to consult the Commissioner before entering into agreements to share the passport database with overseas authorities and empowers the Commissioner to require a review of the agreement from time to time;
- Customs and Excise Act 1996 (s.281) – a similar requirement to the Passports Act 1992 (s.36) for cross-border customs agreements; and
- Corrections Act 2004 (s.182D) – consultation on arrangements for information sharing for supervision of child sex offenders.

### Consultations on complaints handled by other agencies

- Official Information Act 1982 (s.29B), Local Government Official Information and Meetings Act 1987 (s.29A) and Ombudsmen Act 1975 (s.17A) – provides for consultation with the Ombudsmen on access reviews and general complaints; and
- Inspector General of Intelligence and Security Act 1996 (s.12) – consultation on complaints involving intelligence services.

### **Consultations with the Ombudsmen**

The Ombudsmen routinely consult with 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. The Ombudsmen and the Commissioner agree in most situations where privacy is a withholding ground. 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 2008/09 year, this Office received 25 consultations from the Ombudsmen and completed and closed 22.





# 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 may 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; and
- 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); and
- notifying individuals and allowing them time to challenge the decision before any action is taken (section 103).

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 [www.privacy.org.nz/data-matching-introduction](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
CSC	Community Services Card
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 Credit (formerly Family Support Tax Credits)

## The year in information matching

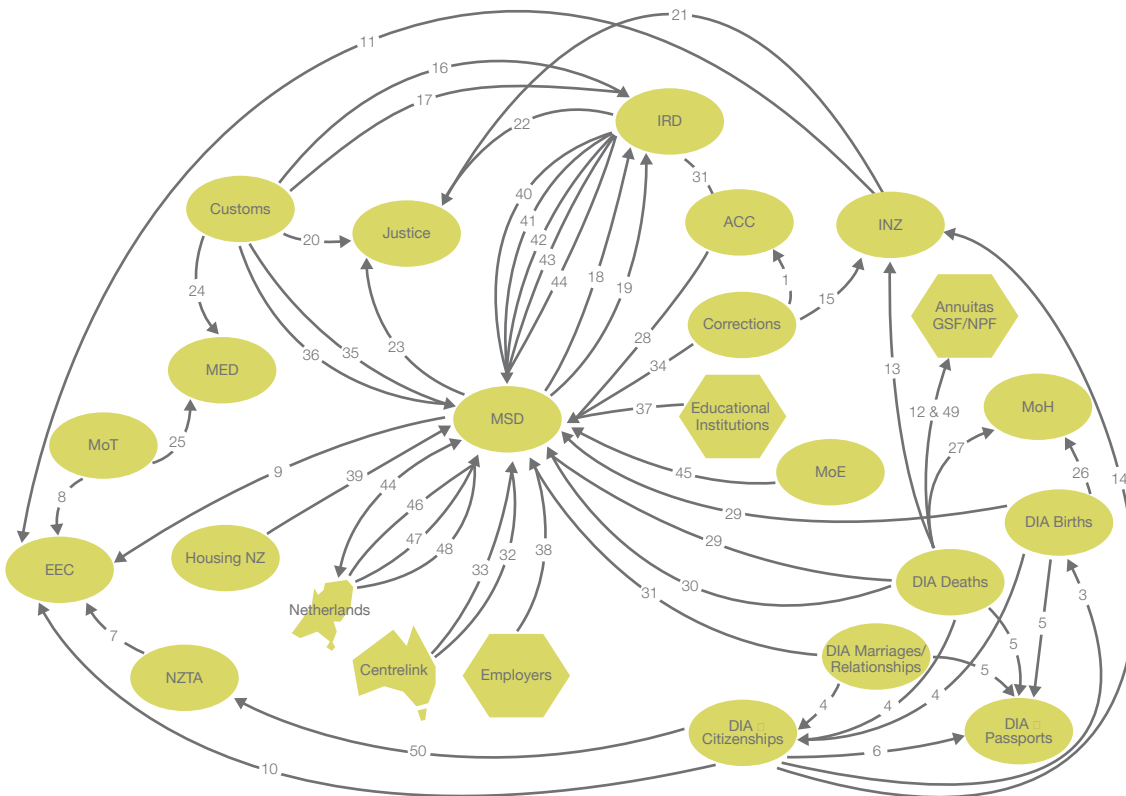
As well as monitoring the activities of the 50 active programmes this year, we have provided assistance and commented on proposals for:

- one new authorisation (currently progressing through Parliament);
- the start of six new matches; and
- numerous changes to match parameters and technical agreements.

Figure 3 shows the flow of information between agencies involved in information matching. This chapter includes an outline of each operating programme, as numbered in the diagram, and an assessment of its compliance.



Figure 3: Active authorised information matching programmes 2008/09



### Electoral Enrolment Centre match activity

The Electoral Enrolment Centre (EEC) has several matching programmes designed to find people who are eligible to be on the electoral roll but are not on it, and one programme to identify people who are on the electoral roll but are not eligible to vote.

The programme to identify ineligible people on the roll has usually been run once a year. In the run up to the 2008 general election, the EEC ran this match on a weekly basis to ensure the roll was as correct as possible.

### Ministry of Health information handling

Amendments to the Births, Deaths, Marriages, and Relationships Registration Act 1995, effective from 24 January 2009, changed the status of several existing programmes so that they became authorised information matching programmes.

As they were pre-existing programmes with pre-existing systems in place, transferring some of these programmes to fit within the information matching framework was not straightforward. This has been particularly difficult for the Ministry of Health (MoH) because its complex matching arrangements and lack of direct contact with the individuals concerned do not readily fit with the need to verify data and limit its retention.

MoH is amending its own processes to put in as many safeguards as are practicable. These were not all in place during this reporting year. We have since been advised by MoH that the agreed

safeguards are now in place. We expect any remaining issues to be fixed in their system re-development, planned for implementation in 2011. We will continue to work with the Ministry to assist them with this.

### **Data security project**

Following several high profile government data breaches overseas in late 2007, we reviewed the handling of files physically transferred on digital media (floppy discs, CDs or tapes) for use in information matching programmes.

Of 46 matching programmes, 19 involved data being transferred physically on unencrypted digital media. By the end of the 2007/08 reporting period, three remained unencrypted. Two of these are now encrypted transfers on USB sticks, but one remains unencrypted (for the IR/ACC Levies and Compensation programme). We expect this data transfer to move to a secure online transfer in the near future.

### **Outreach**

The Office convened two Information Matching Interest Group meetings during the 2008/09 year, where agencies shared their information matching experiences, practices and plans. Both meetings were well attended with a diverse mix of agencies represented.

The Office ran three education workshops focused on information matching and published three editions of the Information Matching Bulletin 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 Information Matching Shared Workspace that was launched in May 2007 has been discontinued. The workspace was not widely used by the interest group and did not warrant the resources required to maintain its operation.

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

Each year we report on the potential number of programmes that have been authorised. However, this is merely our 'best estimate' because, as time passes and programmes become operational, some may be operated as a single programme even though several programmes were anticipated, or vice versa.

Parliament passed five new information matching authorisations during the reporting period. All of these authorisations were in the Births, Deaths, Marriages, and Relationships Registration Amendment Bill (assented 24 July 2008), which amended the Births, Deaths, Marriages, and Relationships Registration Act 1995 (BDMRR).

Section 78A (Schedule 1A) of the BDMRR has been updated, authorising four active programmes. Previously these four matches were each operating under a memorandum of understanding outside the information matching framework. They are:

- BDM (Deaths)/Ministry of Health NHI and Mortality Register Programme;
- BDM (Births)/Ministry of Health NHI and Mortality Register Programme;
- BDM(Deaths)/NPF Eligibility Programme;
- BDM(Deaths)/GSF Eligibility Programme.

The new BDMRR section 78B authorises the Registrar-General to obtain information from MSD to assist in locating and contacting the mothers of children whose births are unregistered, so that their births may be registered. This is not yet an active programme.

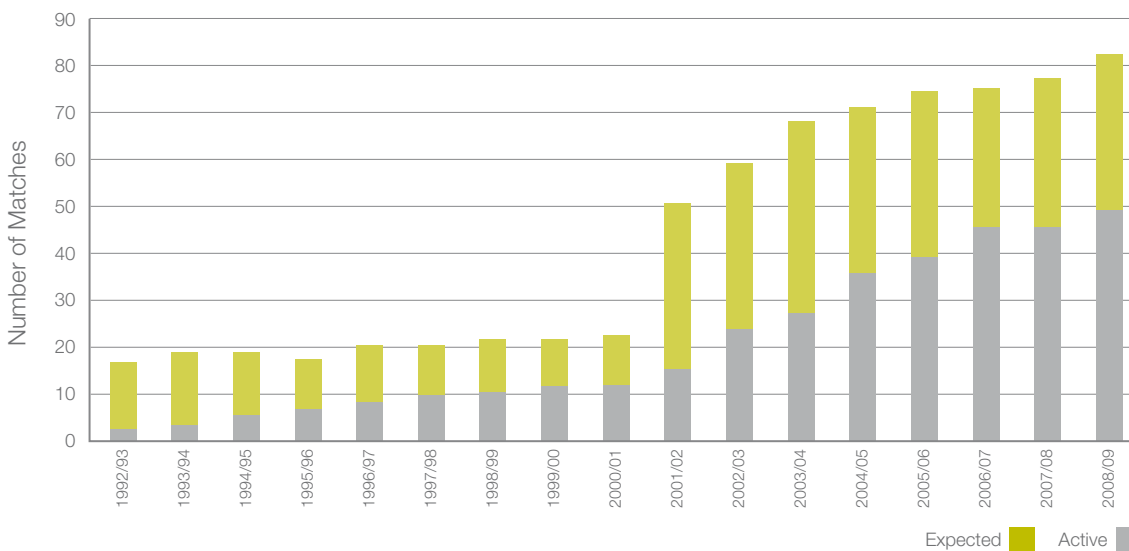
Two programmes authorised in previous years are now active. They are:

- BDM (Deaths)/NZTA Deceased Driver Licence Holders Programme;
- Customs/IR Child Support Alerts Programme.

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

- BDM (Deaths)/Justice (MLC) Maori Land Title Succession Programme;
- BDM (Births)/MoE Student Birth Confirmation Programme.

Figure 4: Authorised and active information matching programmes



### 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 2009, 26 of the 50 active programmes used online transfers. The 11 requests for online transfers, granted by the Commissioner during the 2008/09 year, are listed below. The Commissioner also granted one variation to an existing approval.

**TABLE 14:** SHORT TERM ONLINE APPROVALS 2008/09

User agency Programme name (and number) Approval date	Reason	Grounds
<b>Inland Revenue (IR)</b>		
Child Support Alerts (programme 16) 6 August 2008	Efficiency Technology enabled	Timely delivery of data Improved system integration
Working for Families (programme 18) 29 April 2009	Efficiency Technology enabled	Necessary to enable continuous payments
<b>Ministry of Social Development (MSD)</b>		
Arrivals and Departures (programme 35) 17 December 2008	Efficient use of technology	Enhanced verification process
<b>New Zealand Transport Agency (NZTA)</b>		
Deceased Driver Licence Holders (programme 50) 1 October 2008	Efficiency Technology enabled	Timely delivery of data

**TABLE 15:** LONGER TERM ONLINE APPROVALS 2008/09

User agency Programme name (and number) Approval date	Reason	Grounds
<b>Department of Internal Affairs (DIA)</b>		
Citizenship Application Processing (programme 4) 10 December 2008	Continued efficiency Security	Satisfactory audit result
<b>ACC</b>		
Prisoners (programme 1) 16 June 2009	Efficiency and Security	Satisfactory audit result
<b>Ministry of Economic Development (MED)</b>		
Motor Vehicle Importers (programme 24) 20 May 2009	Continued efficiency	Satisfactory audit result
<b>Immigration New Zealand</b>		
Prisoners (programme 15) 29 May 2009	Continued efficiency	Satisfactory audit result
<b>Ministry of Social Development (MSD)</b>		
Deceased Persons (programme 30) 26 June 2009	Continued efficiency	Satisfactory audit result
Married Persons (programme 31) 26 June 2009	Continued efficiency	Satisfactory audit result enhanced security
Prisoners (programme 34) 26 June 2009	Continued efficiency	Satisfactory audit result

## OPC reporting

We have changed the format of our reports this year so that this printed version contains a more concise account of activities and compliance, without the detailed system descriptions that do not usually change from year-to-year.

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

## 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.

### 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 transferred weekly by online transfer.

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

#### 2008/09 ACTIVITY:

Match runs	40
Records received for matching	77,255
Possible matches identified	668
Overpayments established (number)	49
Overpayments established	\$37,272
Average overpayment	\$760
Challenges	0
Successful challenges	0

**COMMENTARY:** There were only 40 match runs this year. ACC combined some of the 52 weekly files, because of a recurring hardware issue. This issue has been resolved.

Last year ACC proposed 'time taken to identify debts' as a possible additional measure for this programme. ACC is continuing to investigate whether this measure will be useful.

**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 tape.

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

**2008/09 ACTIVITY:**

Self-employed people's records received for matching	493,563
Employers' records received for matching	470,368
Invoices issued to self-employed people	227,379
Invoices issued to employers	265,951
Challenges by individuals	28
Challenges by corporations	28
Total challenges	56
Successful challenges	7

**COMMENTARY:** This programme was previously called the IR/ACC Residual Claims Levies Programme. The name has been changed to better reflect the purpose of the programme. The number of records received for matching has reduced this year because IR has changed their extraction program to exclude duplicates.

**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, parent's 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.

**2008/09 ACTIVITY:**

Births registered	64,366
Notices of adverse action	1,703
Challenges received	378
Successful challenges	305
Citizenship by birth declined	1,398

**COMMENTARY:** DIA is required to provide an annual audit report on the operation of the matching programmes conducted between DIA units and to provide various statistics for the particular programme. However, this year, instead of conducting the audit of the system, DIA management provided a letter advising that there has been no change to the process, and reporting on privacy training activities. This does not meet the annual reporting requirements set for the programme. We therefore had to use the statistical information that DIA gave us to assess the programme.

Successful challenges to the accuracy of the matching process have continued to increase from 11 percent for 2007/08 to 18 percent this year. This means that more than 300 individuals were initially not matched correctly as being eligible for New Zealand citizenship. DIA attributes this to instances of incomplete and inaccurate information on some applications that is clarified when the person is contacted.

**COMPLIANCE:** Compliant, but see the first paragraph of the commentary.

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

**PURPOSE:** To verify a parent's citizenship status if required for the determination of 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 program 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 parent's full names.

**2008/09 ACTIVITY:**

Applications for citizenship by descent (may include more than one person)	6,918
Notice of adverse action (arising from failure to match)	8
Successful challenges	8
Citizenship by descent registered	7,936

Applications may be withdrawn at any stage, or will be declined if eligibility criteria are not met.

**COMMENTARY:** DIA is required to provide an annual audit report on the operation of the matching programmes conducted between DIA units. However, this year, instead of conducting an audit of the system, DIA management provided a letter advising that there has been no change to the process, and reporting on privacy training activities. This does not meet the annual reporting requirements set for the programme. In particular, in the absence of an up to date audit we were initially unable to assess compliance as necessary under the Act. We therefore required DIA to provide us with sufficient statistical information to allow us to assess the programme. DIA did so.

**COMPLIANCE:** Compliant, but see commentary.

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

**PURPOSE:** To verify, by comparing details with the births, deaths and marriages registers, if 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 program 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.

**2008/09 ACTIVITY:**

Passport applications	382,475
Possible matches: Births	797,823
Possible matches: Marriage/Relationships	118,773
Possible matches: Deaths	1,374,962
Notice of adverse action	8,132
Passports issued (diplomatic, official and standard)	387,523

The number of passports issued this period exceeds the number of applications for passports received during this period. This is because passports were issued this year based on applications received last year.

DIA advises that no passports were declined as a direct result of this match. However, if the applicant could not be contacted, for example to supply further information necessary to make a successful match, then their application would lapse after six months. DIA would need to check each cancelled application in order to identify any such cases.

**COMMENTARY:** DIA is required to provide an annual audit report on the operation of the matching programmes conducted between DIA units. However, this year, instead of conducting an audit of the system, DIA management provided a letter advising that there has been no change to the process, and reporting on privacy training activities. This does not meet the annual reporting requirements set for the programme. In particular, in the absence of an up to date audit we were initially unable to assess compliance as necessary under the Act. We therefore required DIA to provide us with sufficient statistical information to allow us to assess the programme. DIA did so.

**COMPLIANCE:** Compliant, but see commentary.

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

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

**YEAR COMMENCED:** 2003

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

**CITIZENSHIP (DIA) DISCLOSURE TO PASSPORTS (DIA):** A computer program identifies possible matches from the Citizenship database. Only details from these possible matches are displayed to Passports staff. These details include full name, date of birth, country of birth and date citizenship was granted.



**2008/09 ACTIVITY:**

Passport applications	382,475
Possible matches to Citizenship records	336,169
Notice of adverse action (arising from failure to match)	1,094
Successful challenges	1,094
Passports issued (diplomatic, official and standard)	387,523

Not all passport applications would require matching to Citizenship records.

DIA advises that no passport applications were declined as a direct result of this match.

**COMMENTARY:** DIA is required to provide an annual audit report on the operation of the matching programmes conducted between DIA units. However, this year, instead of conducting an audit of the system, DIA management provided a letter advising that there has been no change to the process, and reporting on privacy training activities. This does not meet the annual reporting requirements set for the programme. In particular, in the absence of an up to date audit we were initially unable to assess compliance as necessary under the Act. We therefore required DIA to provide us with sufficient statistical information to allow us to assess the programme. DIA did so.

**COMPLIANCE:** Compliant, but see commentary.

## 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, in order that they may be invited to enrol; and
- 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.

**2008/09 ACTIVITY:**

Match runs	4
Records received for matching	597,164
Invitations to enrol sent out	91,299
Invitations presumed delivered	88,475
New and updated enrolments	18,889
Percentage of letters delivered resulting in changes	21%
No response	69,586
Cost	\$64,315.49
Average cost per enrolment	\$3.40

**COMMENTARY:** On 1 August 2008, Land Transport New Zealand (LTNZ) became part of the New Zealand Transport Authority (NZTA). Prior to this change, this programme was known as the LTNZ/EEC Unenrolled Voter Programme.

**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, in order that they may be invited to enrol; and
- 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 extract. The 'Owner ID' reference number is also included to identify any multiple records for the same person.

**2008/09 ACTIVITY:**

Match runs	4
Records received for matching	1,555,608
Invitations to enrol sent out	132,563
Presumed delivered	125,804
New and updated enrolment	24,763
Percentage of letters delivered resulting in changes	20%
No response	101,041
Cost	\$90,468.90
Average cost per enrolment	\$3.65

**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 have not enrolled, in order that they may be invited to enrol; and
- 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.

**2008/09 ACTIVITY:**

Match runs	4
Records received for matching	649,095
Invitations to enrol sent out	110,081
Presumed delivered	106,514
New and updated enrolments	23,629
Percentage of letters delivered resulting in changes	22%
No response	82,885
Cost	\$77,234.39
Average cost per enrolment	\$3.27

**COMPLIANCE:** Compliant.

## 10. Citizenship/EEC Unenrolled Voters Programme

**PURPOSE:** To compare the citizenship register with the contents of 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).

**2008/09 ACTIVITY:**

Match runs	4
Records received for matching	25,138
Invitations to enrol sent out	1,316
Presumed delivered	1,281
New and updated enrolments	252
Percentage of letters delivered resulting in changes	20%
No response	1,029
Cost	\$4,171.98
Average cost per enrolment	\$16.56

**COMMENTARY:** This year EEC identified that the file it received from DIA included multiple records relating to individuals who had several variations of their names entered on the DIA system. After discussion with the Office, EEC and DIA agreed a method of tagging these records without using the DIA's 'client number'.

**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>6</sup>, so their names may be removed from the roll.

**YEAR COMMENCED:** 1996

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

**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.

### 2008/09 ACTIVITY:

Records received for matching	836,161
Possible matches identified	4,217
Notice of adverse action sent	4,217
Challenge received	467
Successful challenges	434
Removals from roll	3,694
Cost	\$167,557
Average cost per removal	\$45.36

**COMMENTARY:** EEC is increasing the frequency with which it obtains the data from INZ to keep the roll as correct as practicable. Previously, it obtained the data once a year. During 2008/09, extracts were obtained in July, then on a weekly basis between 15 September and 14 November 2008 (in the run up to the general election), and once again in June 2009.

Also, EEC used to check with INZ to confirm all 'matched' records. This check is no longer seen to be useful now that data is received more frequently and is therefore up-to-date. Ceasing to conduct this check during 2008/09 reduced the programme's average administrative cost.

**COMPLIANCE:** Compliant.

## 12. BDM(Deaths)/GSF Eligibility Programme

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

**YEAR COMMENCED:** 2009

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

**BDM DISCLOSURE TO GSF:** BDM provides information from the Deaths Register covering the 12 weeks prior to the extract date. The death extract 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).

<sup>6</sup> To enrol in elections, an individual must be a New Zealand citizen or permanent resident.

**2008/09 ACTIVITY:**

Records received for matching	12,013
Possible matches identified	3,517
Notices of adverse action sent	138
Challenges	1
Successful challenges	1

**COMMENTARY:** Amendments to the Births, Deaths, Marriages, and Relationships Registration Act 1995, effective from 24 January 2009, changed the status of this programme to an authorised information matching programme. The programme was previously operating under a memorandum of understanding. This programme report covers the period of operation as an authorised information programme from 1 April 2009 to 30 June 2009.

The one challenge that has occurred during this period was verified as being a mis-match.

**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 Immigration New Zealand (INZ's) database of overstayer and temporary permit holder population.

**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 extract date. The death extract 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.

**2008/09 ACTIVITY:**

Records received for matching	29,119
Possible matches identified	296
Records marked as deceased – overstayer list	145
Records marked as deceased – temporary visa holders' list	83
Total number of records updated as deceased	228

**COMPLIANCE:** Compliant.

### 14. Citizenship/INZ Entitlement to Reside Programme

**PURPOSE:** To identify and remove from the 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.

**2008/09 ACTIVITY:**

Match runs	3
Records received for matching	1,013,867
Possible matches identified	2,663
Number of NZ citizens removed from the overstayer list	428

**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 permits to be in New Zealand have 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.

**2008/09 ACTIVITY:**

Match runs	52
Possible matches identified	340
Cases excluded as not being eligible for removal or deportation	287
Notices of adverse action	53
Successful challenges	1
Cases considered for removal or deportation	46
Removals and deportations from NZ at year end	34

**COMMENTARY:** Last year we reported that INZ wanted to receive offence date information as part of this programme. Corrections and INZ are still discussing how to implement this.

Recent changes to the Sentencing Act 2002 introduced community-based sentences. INZ wishes to include prisoners with these sentences in the programme, but Corrections believes there is no provision to allow this. INZ is reviewing this policy.

Another matching issue identified during this period involved a discrepancy between one individual's sentencing record received in the programme and the relevant sentencing record held by Police. While the match only provided one offence record, which did not identify the prisoner as being potentially liable for deportation, a further check with Police information showed details of three offences, making the prisoner potentially liable for deportation. INZ is reviewing this.

**COMPLIANCE:** Compliant.

## 16. Customs/IR Child Support Alerts Programme

**PURPOSE:** To identify parents in serious default<sup>7</sup> 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, date and 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).

**2008/09 ACTIVITY:**<sup>8</sup>

Possible matches identified	6,928
Arrival cards received for liable parents	1,219
Number of liable parents	917
Number of liable parents where contact has been made	732
New contact details updated	394
Existing contact details confirmed	332
Contact details not useful	191
Cards that did not meet the matching criteria	22

An audit on the operation of this programme found there were 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 all student loan borrowers.

**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.

**2008/09 ACTIVITY:** Approximately 54,400 student borrower records were updated as a result of matching student borrower records with travel movement information held by Customs.

7. **Serious default** means having an amount of financial support debt due and owing to the Commissioner of Inland Revenue and satisfying criteria agreed by the Commissioner and the Privacy Commissioner in consultation with the Customs' Chief Executive (Customs and Excise Act 1996, s.280J).

8. Activity for this programme is for the 12 months from 1 September 2008 to 31 August 2009.

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

**COMPLIANCE:** Compliant.

## 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. 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.

**2008/09 ACTIVITY:** MSD and IR jointly distributed \$2,673 million in WFFTCs during 2008/09, with 203,000 people receiving an average \$156 weekly payment from IR as at June 2009.

An audit on the operation of this programme found there were effective controls in place and no issues were identified. However, a separate audit of the online transfer system revealed some issues (see commentary).

**COMMENTARY:** An audit on the online transfer system contained two key findings. Firstly, the Technical Standards Report governing the operation of the programme had not been updated to reflect the online transfer approval issued by the Privacy Commissioner. Secondly, security access to the MSD file was set to read-write instead of the required read-only access, providing an opportunity for fraudulent activity.

However, there was no evidence that any fraudulent activity had occurred and changes to remedy the adverse audit findings have been completed. Given the nature of the information transferred in this programme and the adverse audit findings, a new approval with a shorter review period was granted.

**COMPLIANCE:** Compliant, but technical issues identified – see commentary.

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

**PURPOSE:** To identify individuals who have wrongly received WFFTCs from both MSD and IR.

**YEAR COMMENCED:** 1995

**FEATURES:** Data transferred up to 26 times a year by tape.

**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, date tax credits payments started and amount paid.

**2008/09 ACTIVITY:** Despite the operation of this programme, WFFTC debt increased by 17.8 percent to \$200 million during the reporting year. Incorrect payments can readily occur for people whose income fluctuates during the year and the estimated annual income, used to establish weekly or fortnightly payment levels, is less than the actual income they earned for the year.

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

**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; or
- court imposed fines of \$5,000 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 \$1,000 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.

**2008/09 ACTIVITY:**

Silent alerts triggered	1,821
Individuals subject to silent alerts <sup>9</sup>	976
Intercept alerts triggered	79
Total number of people intercepted <sup>10</sup>	65
On departure	55
On arrival	12
Total incorrect intercepts	6
Fines had already been paid	1
Wrong person identified by the match	5
Interception not completed	4
Fines received	\$106,465
Reparation received	\$121,877
Amount under a current time to pay arrangement	\$212,614
Remittals/alternative sentence imposed	\$115,759

Last year we reported that Justice had carried out a review of the Collection of Fines at Airports (CoFaA) project, which identified several issues with their procedures.

The main problems we reported were that multiple sources of instructions existing within the Ministry of Justice contributed to issues in the management of identity, the interception of fines defaulters no longer subject to an alert, and errors in reports to the Privacy Commissioner.

The review of CoFaA recommended that Justice make procedural changes to resolve those issues. This year, Justice reports that:

- it has consolidated all CoFaA documentation and has centralised CoFaA operations to a dedicated team;
- the CoFaA Operational Working Group meets quarterly, creating closer inter-agency working relationships; and
- there have been no delays to aircraft because of CoFaA alerts since new processes were implemented.

**COMPLIANCE:** Compliant.

## 21. INZ/Justice Fines Defaulters Tracing Programme

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

**YEAR COMMENCED:** 2006

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

9. See the INZ/Justice Fines Defaulters Alerts Programme report for details of actions taken.

10. The number of alerts on arrival or departure will not necessarily equal the total number of people intercepted because a person can trigger multiple alerts in a given period.

**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).

**2008/09 ACTIVITY:**

Records sent to INZ	1,820
Notices of adverse action	747
Successful challenges	0
Payment received for fines	\$625,134
Amounts under a current time-to-pay arrangement	\$787,652
Remittals/alternative sentence imposed	\$258,308

**COMPLIANCE:** Compliant.

## 22. IR/Justice Fines Defaulters Tracing Programme

**PURPOSE:** To enable the Ministry of Justice 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.

**2008/09 ACTIVITY:**

Match runs	7
Records sent for matching	129,476
Possible matches identified	36,129
Notices of adverse action <sup>11</sup>	23,102
Challenges	50
Successful challenges	22
Collection instituted	10,174
Amount paid or settled <sup>12</sup>	\$5,905,868

11. An enhancement to reporting from 1/7/2008 means that Justice now records the actual number of letters sent rather than the number of people eligible to be sent a notice.

12. This is an 'in-progress' figure because payments are attributed to this programme for 12 months after the match run date. Final collection figures will be published on our website when they become available.

**COMMENTARY:** There were significantly fewer records sent for matching during the 2008/09 year than previously (129,476 compared with 343,200 in 2007/08). Justice believes this was because more fine defaulter records were already under other tracing action and therefore not available for matching.

**COMPLIANCE:** Compliant

### 23. MSD/Justice Fines Defaulters Tracing Programme

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

**YEAR COMMENCED:** 1998

**FEATURES:** Data transferred up to 13 times a 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.

**2008/09 ACTIVITY:**

Match runs	5
Records sent for matching	70,941
Possible matches identified	4,890
Notices of adverse action <sup>13</sup>	3,584
Challenges	5
Successful challenges	1
Collection instituted	2,056
Amount paid/remitted <sup>14</sup>	\$1,363,620

**COMMENTARY:** There were significantly fewer records sent for matching during the 2008/09 year than previously (70,941 compared with 353,404 in 2007/08). Justice believes this was because more fine defaulter records were already under other tracing action and therefore not available for matching.

**COMPLIANCE:** Compliant

### 24. Customs/MED Motor Vehicle Traders Importers Programme

**PURPOSE:** To enable the Ministry of Economic Development (MED) 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.

13. An enhancement to reporting from 1/7/2008 means that Justice now records the actual number of letters sent rather than the number of people eligible to be sent a notice.

14. This is an 'in-progress' figure because payments are attributed to this programme for 12 months after the match run date. Final collection figures will be published on our website when they become available.

**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.

**2008/09 ACTIVITY:**

Match runs		4
Records received for matching		249
Individuals or entities of interest identified		64
Notices of adverse action sent		96 <sup>15</sup>
Successful challenges	Entities: registered under another name	1
	Entities: primary purpose not financial gain	19
Entities referred to the National Enforcement Unit		0
Registrations as a result of notices of adverse action		6

**COMMENTARY:** An internal audit of the online transfer system revealed that while information sent from Customs to MED was properly secured, transfers from MED to Customs were unsecured because a security feature was not properly enabled. MED immediately remedied this oversight and no data breaches occurred.

As anticipated, after five years of operation there has been a considerable reduction in new individuals or entities received by MED for matching. The programme now operates quarterly (formerly monthly).

**COMPLIANCE:** Compliant, but technical issues identified – see commentary.

## 25. MoT/MED Motor Vehicle Traders Sellers Programme

**PURPOSE:** To enable MED 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:** MoT provides MED with the full name, date of birth and address of all individuals or entities that 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.

<sup>15</sup>. This includes 32 second notices sent during the reporting period.

**2008/09 ACTIVITY:**

Match runs		4
Records received for matching		1,647
Individuals or entities of interest identified		600
Notices of adverse action sent		684 <sup>16</sup>
Successful challenges	Entities: registered under another name	6
	Entities: primary purpose not financial gain	393
Entities referred to the National Enforcement Unit		0
Registrations as a result of notices of adverse action		77

**COMPLIANCE:** Compliant

## 26. BDM (Births)/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 provided monthly on CD.

**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.

**2008/09 ACTIVITY:**

Records received for matching (since 25 January 2009)	33,194
Possible matches identified	33,146
Records not matched	48

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

**COMMENTARY:** Amendments to the Births, Deaths, Marriages, and Relationships Registration Act 1995, effective from 24 January 2009, changed the status of this programme to an authorised information matching programme. The programme was previously operating under a memorandum of understanding.

MoH has not retained birth records received after 24 January 2009 if there was no match.

However, MoH has retained birth records received before 24 January 2009 where there was no match. We have some concern about this retention because, over time, DIA may need to make changes to individuals' identity records. Therefore, old birth records may not match to an individual's current identity.

<sup>16</sup>. This includes 84 second notices that were sent during the reporting period.

Another concern is that MoH currently does not verify the results of the match before updating its records. MoH does take considerable steps to ensure its matching is accurate, but the Ministry does not verify the results of the match with the individuals concerned. Downstream users can modify this data if they become aware of a discrepancy. However this widespread ability to change core data can present other accuracy and privacy problems. MoH's system re-development, planned for implementation in 2011, should fix any remaining practical and privacy issues.

**COMPLIANCE:** Compliant, but see comments above.

## 27. 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.

### 2008/09 ACTIVITY:

Records received for matching (since 25 January 2009)	13,755
Possible matches identified	12,024
Records not matched	1,668
New NHIs allocated	63
Corrections to matches (including from previous years matches)	12

**COMMENTARY:** Amendments to the Births, Deaths, Marriages, and Relationships Registration Act 1995, effective from 24 January 2009, changed the status of this programme to an authorised information matching programme. The programme was previously operating under a memorandum of understanding.

It is our view that some MoH practices have not complied with all the information matching provisions. We have been encouraging MoH to update these practices.

In particular, MoH makes the NHI available to other agencies (such as DHBs) which may then rely on the information even though the recorded deaths have not been verified. MoH has not been verifying the death matching as MoH has no direct interaction with the individuals or any mechanism to do so. MoH has advised that after the end of this reporting period it modified its system to notify downstream users of NHI information that the death has not been verified. This will reduce the chances that adverse action will be taken against individuals who are incorrectly notified as deceased on the NHI.

MoH has also amended its own process, from June 2009, to check two registers they administer, the National Booking System and the National Immunisation Register, for possible matches, before the NHI is updated. Where matches are found with these registers verification of the death is sought. This reduces the risk of people being removed from these registers in error. MoH has undertaken to investigate if it maintains any other registers which can also be checked.

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

## 28. 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:

- current claims that have continued for two months since the first payment;
- claims where there has been no payment made to the claimant for six weeks; or
- 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.

**2008/09 ACTIVITY:**

<b>New match runs started in the reporting period</b>	
Match runs	52
Records received for matching	2,469,022
Possible matches identified	7,124
<b>All match runs active in the reporting period<sup>17</sup></b>	
Matches that required no further action	4,702
Notices of adverse action	2,536
Challenges	158
Successful challenges	81
Overpayments established	1,370
Value of overpayments established	\$1,735,763

A jump in challenges and successful challenges occurred because of a one-off incident where incorrect data was received from ACC. The information received related to historic injuries and was not related to periods where the individuals were in receipt of concurrent ACC and MSD payments. Once MSD identified the issue, it was able to identify the clients affected and cease any further action.

**COMPLIANCE:** Compliant.

## 29. BDM/MSD Identity Verification Programme

**PURPOSE:** To confirm the validity of birth certificates used by clients when applying for financial assistance, and also to verify that clients were not on the New Zealand Deaths' Register.

**YEAR COMMENCED:** 2007

**FEATURES:** The programme operates daily using data transferred by CD every quarter.

<sup>17</sup>. This includes activity from match runs initiated in the previous year.



**BDM DISCLOSURE TO MSD:** BDM provides birth and death information covering the period of 90 years prior to the extract 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.

**2008/09 ACTIVITY:**

Benefit applications processed	489,214
Possible matches identified	21,582
Matches that required no further action	5,417
Letters advising update of information	2,051
Notices of possible adverse action	54
Challenges	0
Overpayments established	1
Value of overpayments established	\$28.39
Cases referred for further investigation	7

**COMMENTARY:** To reduce the processing time and costs of this programme, MSD has limited the records included in the programme to applications where an ongoing benefit has been granted. Prior to February 2009, all benefit applications were included in the programme, including those for small one-off payments.

**COMPLIANCE:** Compliant.

### 30. 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 extract date. The death details include the full name, gender, birth date, death date, home address, death registration number and spouse's full name.

**2008/09 ACTIVITY:**

<b>New match runs started in the reporting period</b>	
Match runs	52
Records received for matching	29,457
Possible matches identified	8,589
<b>All match runs active in the reporting period</b>	
Matches that required no further action	6,418
Notices of adverse action	2,171
Challenges	0
Overpayments established	459
Value of overpayments established	\$330,203

A big drop in the number of possible matches identified was a result of improvements to the match filtering process introduced in November 2008. However, the number of notices of adverse action and overpayments established remained about the same as the 2007/08 year.

**COMPLIANCE:** Compliant.

### 31. BDM (Marriages)/MSD Married Persons Programme

**PURPOSE:** To identify current clients who have married, so that MSD can update client records and reassess 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 extract 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.

**2008/09 ACTIVITY:**

<b>New match runs started in the reporting period</b>	
Match runs	52
Records received for matching	23,378
Possible matches identified	2,646
<b>All match runs active in the reporting period</b>	
Matches that required no further action	1,572
Notices of adverse action	1,085
Challenges	2
Successful challenges	1
Overpayments established	498
Value of overpayments established	\$515,537

**COMPLIANCE:** Compliant.

### 32. Centrelink/MSD Change in Circumstances Programme

**PURPOSE:** This programme 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.

**2008/09 ACTIVITY:**

Changes of information received by MSD from Centrelink	543,624
Notices of adverse action	4,742
Changes of information sent by MSD to Centrelink	161,430

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

**COMPLIANCE:** Compliant.

### 33. 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 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, as derived from arrival and departure information.

**2008/09 ACTIVITY:**

Records sent for matching (1 July 2008 to 31 March 2009)	8,770
Australian pensions granted	2

No records were extracted from April to June due to a software upgrade. This has since been completed.

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

**COMPLIANCE:** Compliant.

### 34. 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 extract file. Details disclosed include the full name (including aliases), date of birth, prisoner unique identifier and prison location, along with incarceration date, parole eligibility date and statutory release date.

**2008/09 ACTIVITY:**

<b>New match runs started in the reporting period</b>	
Match runs	321
Records received for matching	10,261,871
Possible matches identified	14,801
<b>All match runs active in the reporting period</b>	
Matches that required no further action	7,260
Notices of adverse action	7,520
Challenges	16
Successful challenges	11
Overpayments established	2,233
Value of overpayments established	\$443,786

**COMMENTARY:** There has been a dramatic increase in the number of records disclosed by Corrections to MSD. This is because changes were made to the programme in November 2008, including:

- all prisoners on muster are now included in the match rather than just new arrivals;
- all prisoner alias names are included, linked to their true name to reduce the possibility that an innocent person’s benefit is suspended; and
- the programme has been extended to match against MSD’s student records, following the discovery that prisoners were fraudulently accessing the Government’s student loan scheme.

MSD’s total overpayments have dropped by about 75 percent, from an annual average of \$1.8 million, because MSD now immediately suspends benefits without waiting for a response to the notice of adverse action<sup>18</sup>. This change in process aims to reduce prisoner debt levels and their impact on prisoner rehabilitation.

**COMPLIANCE:** Compliant.

18. Authority to immediately suspend a benefit prior to sending a notice of adverse action for this programme was authorised by legislation in April 2008 and implemented in May 2008.

### 35. 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 extract date. Each travel movement record includes the traveller's full name, date of birth, gender, travel document number, country code and flight details.

**2008/09 ACTIVITY:**

<b>New match runs started in the reporting period</b>	
Match runs	52
Records received for matching	9,093,528
Possible matches identified	31,092
<b>All match runs active in the reporting period</b>	
Matches that required no further action	18,635
Notices of adverse action	10,901
Challenges	80
Successful challenges	70
Overpayments established	5,800
Value of overpayments established	\$6,248,204

**COMMENTARY:** In December 2008, the Privacy Commissioner granted an online transfer approval authorising specialist MSD staff to access Customs passenger movement information via a web-based interface. This allows MSD to verify the results of the programme more efficiently.

The number of successful challenges appears high, however they represent only a small proportion of the total programme activity.

**COMPLIANCE:** Compliant.

### 36. Customs/MSD Periods of Residence Programme

**PURPOSE:** To enable MSD 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.

**2008/09 ACTIVITY:** MSD staff accessed 178 Customs records.

**COMMENTARY:** An audit found no inappropriate use of the online access and concluded that the programme complied with the information matching requirements.

**COMPLIANCE:** Compliant.

### 37. 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; and
- 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 that have not developed systems to handle batches of data appropriately.

**MSD STUDYLINK 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.

**2008/09 ACTIVITY:**

Educational institutions involved in the matching programme	582
Records sent for matching	829,172
Individual applications involved in matching	213,665
Notices of adverse action sent out (individuals may receive more than one)	41,211
Percentage of applicants issued a notice of adverse action	19%
Challenges <sup>19</sup>	156
Successful challenges	69
Decisions to decline loan/allowance	21,849

**COMMENTARY:** The percentage figure overstates the number of applicants who received notices of adverse action because some applicants received more than one notice.

The number of successful challenges appears high, however they represent only a small proportion of the total programme activity.

**COMPLIANCE:** Compliant.

<sup>19</sup> Includes applications for reviews that were subsequently withdrawn or that were still under consideration at time of reporting.

### 38. Employers/MSD Section 11A Social Security Act Programme

**PURPOSE:** To identify people who are receiving benefits from MSD while in paid employment.

**YEAR COMMENCED:** 1993

**FEATURES:** The programme is conducted on an ad hoc basis and data is transferred manually. (Currently suspended.)

**EMPLOYERS DISCLOSURE TO MSD:** Employers who are likely to have significant numbers of transitory employees are selected for review by MSD regional offices. The selected employers are required to provide the full names, addresses and IRD numbers of their employees.

**2008/09 ACTIVITY:**

Matches approved	1
Matches completed	1
Records received for matching	23
Cases investigated	0
Benefits cancelled or adjusted	0
Total cost	\$175.31
Notices of adverse action sent	0
Challenges	0

**COMMENTARY:** Processing of the one match initiated in 2007/08 was completed, otherwise this match remains suspended by MSD.

**COMPLIANCE:** Compliant.

### 39. HNZ/MSD Benefit Eligibility Programme

**PURPOSE:** To enable MSD detect:

- 'double-dipping' for accommodation assistance;
- differences in information concerning personal relationships, dependent children and tenant income; and
- 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 borders), 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 details provided on termination of the tenancy.

**2008/09 ACTIVITY:**

<b>New match runs started in the reporting period</b>	
Match runs	53
Records received for matching	94,649
Possible matches identified	7,185
<b>All match runs active in the reporting period</b>	
Matches that required no further action	6,986
Notices of adverse action	139
Challenges	0
Overpayments established (number)	84
Overpayments established (dollars)	\$71,281

Fewer possible matches were identified during the 2008/09 year compared with the previous year because of the improved filtering process initiated during 2007/08. The programme continues to identify only a small fraction of the forecasted<sup>20</sup> \$1.4 million in annual overpayments.

**COMPLIANCE:** Compliant.

## 40. IR/MSD Commencement/Cessation Benefits Programme

**PURPOSE:** To detect those who are receiving a benefit and working at the same time.

**YEAR COMMENCED:** 1993

**FEATURES:** Data is transferred online up to six times a 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 previous match;
- had cancelled benefits included in the previous match run and did not return any employment details for Inland Revenue;
- were nominated because of some suspicion; or
- 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 full name, date of birth, MSD client number and IRD number, employer name, address, email and phone contact details, employment commencement and cessation dates, and income amount.

20. Information Matching Privacy Impact Assessment 2005, prepared by MSD.



**2008/09 ACTIVITY:**

<b>New match runs started in the reporting period</b>	
Match runs	6
Records received for matching	154,592
Possible matches identified	29,213
<b>All match runs active in the reporting period</b>	
Matches that required no further action	15,029
Notices of adverse action	13,841
Challenges	633
Successful challenges	134
Overpayments established	4,619
Value of overpayments established	\$6,390,325

**COMMENTARY:** The number of successful challenges appears high, however they represent only a small proportion of the total programme activity.

**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 5,000 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 name, address, email and phone contact details, employment commencement and cessation dates, and income amount.

**2008/09 ACTIVITY:**

<b>New match runs started in the reporting period</b>	
Match runs	11
Records received for matching	55,000
Possible matches identified	27,639
<b>All match runs active in the reporting period</b>	
Matches that required no further action	8,567
Notices of adverse action	19,090
Challenges	513
Successful challenges	200
Overpayments established	6,163
Value of overpayments established	\$4,278,836

**COMMENTARY:** The number of successful challenges appears high, however they represent only a small proportion of the total programme activity.

**COMPLIANCE:** Compliant.

## 42. IR/MSD Community Services Card Programme

**PURPOSE:** To identify people who, by virtue of their level of income and number of children, qualify for a Community Services Card (CSC) 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 encrypted USB stick.

**IR DISCLOSURE TO MSD:** For individual tax payers who have received family support tax credits, 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 Working For Families Tax Credits (WFFTC).

**2008/09 ACTIVITY:**

Match runs	52
Records received for matching <sup>21</sup>	2,639,393
CSCs automatically renewed <sup>22</sup>	422,379
'Invitation to Apply' forms sent out	110,855
Notices of adverse action	37,751
Challenges	240
Successful challenges	0

**COMPLIANCE:** Compliant.

21. Including records with change in income information requiring eligibility to be reassessed.

22. These figures do not include cards automatically issued to students based on a match between StudyLink and Work and Income.

### 43. IR/MSD Debtors Tracing Programme

**PURPOSE:** To provide contact details of debtors with whom MSD has lost contact, so as to enable MSD to recover benefit overpayments.

**YEAR COMMENCED:** 1994

**FEATURES:** Data is manually transferred every two months.

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

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

**2008/09 ACTIVITY:**

Match runs	6
Records sent for matching	191,787
Matches potentially useable <sup>23</sup>	65,876
Notices of adverse action	3,255
Debt pursued (from letters presumed delivered)	\$11,371,042
Repayments received by 30 June 2009	\$254,601
Total variable costs incurred <sup>24</sup>	\$103,504

**COMMENTARY:** The data is transferred on encrypted memory sticks. Previously it was securely couriered on unencrypted tapes.

**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 is provided manually, as required.

**IR DISCLOSURE TO THE 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 (SVB) (social insurance) or Uitvoeringsinstituut Werknemers Verzekeringen (UWV) (employee insurance). MSD acts as a liaison point, forwarding valid requests to IR and forwarding the response to the Netherlands.

**2008/09 ACTIVITY:** During 2008/09, 55 requests for information were received and forwarded to IR, and the subsequent responses passed back to the Netherlands.

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

**COMPLIANCE:** Compliant.

23. Useable information is information that is different to that held by MSD. It may not be current and may prove to be unusable.

24. Variable costs are those directly related to the volume of activities undertaken as a result of each match run. Fixed costs such as programme development costs are not included.

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

**PURPOSE:** To verify the results of study information so that MSD can confirm a student's entitlement to a student allowance. In particular, the information derived from this programme enables MSD to:

- detect ineligibility;
- prevent the ongoing payment of assistance for which the recipient is not eligible; and
- establish a debt against the person for the period for which the recipient was ineligible.

**YEAR COMMENCED:** 2006

**FEATURES:** Data transferred daily by online transfers.

**MSD STUDYLINK DISCLOSURE TO MOE:** StudyLink provides MoE 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.

**2008/09 ACTIVITY:**

Records sent for matching	60,164
Individual applications involved in matching	43,963
Notices of adverse action sent out	3,757
Successful challenges	1,163

While the number of successful challenges appears high, the rate is a similar proportion to the previous (full) year. 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.

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

**NETHERLANDS DISCLOSURE TO MSD:** Netherlands SVB responds with the SVB reference number.

**2008/09 ACTIVITY:** As an indicator of activity, MSD issued 264 notices of adverse action in 2008/09. This figure includes some corrections to the SVB reference numbers. There were no challenges to these notices.

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

**COMPLIANCE:** Compliant.

## 47. Netherlands/MSD Debt Recovery Programme

**PURPOSE:** To enable New Zealand and the Netherlands to recover benefit overpayment debts owed to them by individuals living in the other country.

**YEAR COMMENCED:** 2003

**FEATURES:** Data is transferred as required, using an agreed form.

**NETHERLANDS DISCLOSURE TO MSD:** For Netherlands beneficiaries who have received an overpayment from the SVB, the SVB provides MSD with the names, addresses, dates of birth, amount of debts and the Netherlands unique identifiers and MSD client numbers.

**2008/09 ACTIVITY:** This programme did not operate during 2007/08 or 2008/09 because no requests were received from the Netherlands.

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

**COMPLIANCE:** Compliant.

## 48. 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 THE NETHERLANDS:** For MSD clients in receipt of both New Zealand and Netherlands pensions, MSD provides the 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.

**2008/09 ACTIVITY:** During 2008/09, MSD made deductions from pension payments to 3,552 people. There were 1,066 MSD clients resident in the Netherlands.

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

**COMPLIANCE:** Compliant.

## 49. BDM (Deaths)/NPF Eligibility Programme

**PURPOSE:** To identify members or beneficiaries of the National Provident Fund (NPF) 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 extract date. The death extract 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).

**2008/09 ACTIVITY:**

Records received for matching	12,116
Possible matches identified – Pensioners	82
Possible matches identified – Contributors	24
Notices of adverse action sent	106
Challenges	0

**COMMENTARY:** Amendments to the Births, Deaths, Marriages, and Relationships Registration Act 1995, effective from 24 January 2009, changed the status of this match to an authorised information matching programme. The match was previously operating under a memorandum of understanding. This programme report covers the period of operation as an authorised information match from 1 April 2009 to 30 June 2009.

**COMPLIANCE:** Compliant

## 50. 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 extract 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.

**2008/09 ACTIVITY:**

Match runs	19
Records received for matching	20,073
Possible matches identified	11,238
Notices of adverse action	8,156
Challenges	1
Successful challenges	0
Courtesy letters sent <sup>25</sup>	2,398
Driver licence records cancelled	10,559

**COMMENTARY:** A one-off historic match covering deaths that occurred between 1 January 1987 and 30 September 2008 was initiated in March 2009. Processing is still in the early stages because of the large number (600,000) of records involved.

**COMPLIANCE:** Compliant.

25. Where the cancellation of a licence record is not considered to be an adverse action, but is still the result of a recent death, NZTA sends out a courtesy letter advising the estate that the licence record is being cancelled.



# 6: FINANCIAL AND PERFORMANCE STATEMENTS



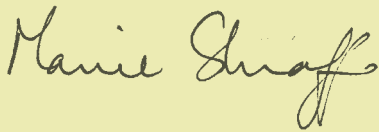
## Statement of responsibility

FOR THE YEAR ENDED 30 JUNE 2009

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 2009.



Privacy Commissioner  
M Shroff  
30 October 2009



General Manager  
G F Bulog  
30 October 2009

## 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 2009

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. 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 2009.

### Unqualified Opinion

In our opinion:

- The financial statements of the Privacy Commissioner on pages 97 to 121:
  - comply with generally accepted accounting practice in New Zealand
  - fairly reflect:
    - the Privacy Commissioner's financial position as at 30 June 2009
    - 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 86 to 96:
  - 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 2009, 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 2009 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 Institute of Chartered Accountants of New Zealand.

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 2008/09

### 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. The Privacy Commissioner has actively supported and contributed to the ongoing review of privacy being undertaken by the Law Commission.
Review of the Privacy Act <ul style="list-style-type: none"><li>• Assist Ministry of Justice in pursuing a finding from the European Union that New Zealand law offers an "adequate" standard of data protection</li><li>• Support Ministry of Justice work on the review of the Act and proposed legislative change process</li></ul>	Achieved. The Privacy Commissioner provided input and support to the Ministry of Justice in the preparation of the Privacy (Cross-border Information) Amendment Bill introduced to Parliament in July 2008 and referred to Select Committee for public consultation. Met with European Commission Officials in October and responded to questions raised by the Officials. The Privacy Commissioner has supported the review of the Act being undertaken by the Law Commission.
Issue and keep current codes of practice	Achieved. Amendment to the Justice Sector Unique Identifier Code issued in December 2008. Convened a reference group of stakeholders from both industry and civil society, and undertook a review of 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.

Significant successes achieved on a number of projects, to better protect privacy and mitigate privacy impacts while agencies still attained, sought policy objectives. Examples include:

- Anti Money Laundering and Financing of Terrorism Bill;
- Immigration Bill;
- Vehicle Confiscation and Seizure Bill;
- Summary Proceedings Amendment Bill;
- Education Amendment Bill;
- Electronic Identity Verification Bill; and
- Guidance provided to agencies, for example, the guidance material on the use of Portable Storage Devices (PSDs).

Provide specialised assistance to government Departments or Ministries in accordance with agreed memoranda of understanding (MOU)

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 State Services Commission, specialised assistance was provided to the SSC and DIA on the privacy impacts of proposed online authentication (the 'Identity Verification Service').

Research work completed on information sharing within government, funded by an MOU with Ministry of Social Development.

Provide assistance to improve whole of government compliance with information matching controls

Achieved.

The Privacy Commissioner granted 10 requests for online transfers across government during the 2008/09 year.

The Office maintains the Information Matching Interest Group. Meetings/seminars were held in August and March covering a wide range of topics.

Ran two education workshops on information matching.

Three Information Matching bulletins were published during the year.

The Office is an observer member of the Cross-Government Biometrics Working Group.

---

Contribute to international initiatives to facilitate cross-border co-operation in privacy standard setting and enforcement

Achieved.

Assisted to develop the OECD Recommendations on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy.

Assisted government agencies to develop a mechanism for inclusion in the Privacy (Cross-border Information) Amendment Bill.

## 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

Achieved.  
Amendment to Justice Sector Unique Identifier Code presented for public submission.

---

All issued codes are referred to the Regulations Review Committee of the House of Representatives

Achieved.  
Amendment to Justice Sector Unique Identifier Code referred to the Regulations Review Committee of the House of Representatives.

---

Assistance provided to government agencies which presents a clear, concise and logical argument, with assumptions made explicit and supported by facts

Achieved.  
Provided advice and assistance to government agencies, in particular Ministry of Health, Ministry of Social Development and the State Service Commission.  
Evidenced through continuation of Memorandum of Understanding with Departments following reviews of activities for previous year.

---

Respond to feedback obtained from recipients of advice

Achieved.  
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 Office is gaining a clear understanding of the objectives an agency is seeking and the policy justifications for those goals.

### Timeliness

Codes of practice meet the agreed timelines for release and implementation

Give advice within a time span that will enable it to be useful to the recipient or within agreed timeframes

### Achievement

Achieved.

Amendment to Justice Sector Unique Identifier released December 2008 in accordance with agreed timelines.

Achieved.

Legal and Policy Team has a focus on being engaged with the early stages of policy and legislative development by agencies, as this is the stage where privacy protective changes can more readily be achieved.

Working to external timeframes and deadlines is standard. The majority of the draft Cabinet Papers and draft Bills received by the Legal and Policy Team have tight timelines for responses. Effective work prioritisation means that extensions to those timelines are rarely sought by the Office.

## Output 2 – Communications

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
- privacy as a human right and develop an awareness of privacy issues.

### Quantity

Organise New Zealand Privacy Awareness Week as part of the Asia-Pacific Privacy Awareness Week

### Achievement

Achieved.

The Office undertook two Privacy Awareness Weeks, the additional Week in May 2009 being to align activities with the preferred dates of overseas jurisdictions for future years.

A wide range of events involving different audiences supported the Weeks. Organisations in public and private sectors ran their own events and over 40 media enquiries were received across the Weeks, including several high-profile stories.



Undertake speaking engagements	<p>Achieved.</p> <p>The Commissioner and her staff provided 35 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 over 200 media enquiries.</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>The Information Matching Interest Group and IM workshops provide good assistance/training in compliance with information matching standards and rules.</p> <p>The results of the PSD Survey also provide useful assistance on risk management to policy makers and others in government.</p>
Contribute to Law Commission Privacy Review	<p>Achieved.</p> <p>The Office attends regular meetings with the Law Commission.</p> <p>Study papers presented to date by the Law Commission have incorporated significant input and comment by the Office.</p> <p>The contribution of the Privacy Commissioner and staff is acknowledged in the published reports of the Law Commission.</p>
Participate in international fora	<p>Achieved.</p> <p>Active participation in the 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

Achieved.

Active participation in Privacy Officer networks.

Established Privacy Officer portal on website to improve interaction and support with Privacy Officers.

---

Undertake a programme of education workshops to promote awareness and understanding of and compliance with the Privacy Act

Achieved.

The Office conducted 60 workshops in this financial year, either on its own premises or visiting individual agencies. This includes workshops out of Auckland and Wellington, including Christchurch, Nelson, Hamilton and Palmerston North.

---

Provide a free enquiries service including 0800 helpline and website access to information, supporting self-resolution of complaints

Achieved.

The enquiries service handled 6,636 enquiries during this financial year, via the 0800 helpline, email and correspondence. In addition the website is available as the first port of call for many people, providing a wide range of information.

---

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.

Establishment of a forum for Privacy Officers only was incorporated into the site.

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 August 2008.

Activities	Estimation	Achieved
Education workshops	60	60
Presentations at conferences/seminars	10	35
Projected number of enquiries received and answered	6,000	6,632
Case notes produced	20	23
Information matching workshops	1	2
Technology and Policy Forums	6	6

Quality	Achievement
Meet internal professional standards	Achieved.
Act on feedback obtained from recipients of advice	Achieved.
Evaluations show that the expectations of 90% of attendees at workshops were 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 98% of instances.
Publications and information are legally accurate	Achieved. We have new publications externally peer reviewed, as well as internally checked.
Case Notes conform with the regional standards adopted by the Asia Pacific Privacy Authorities (APPA)	Achieved. 23 Case Notes were published on our website and made available through websites of overseas jurisdictions who are members of APPA.
Meetings held with, or presentations made to, at least 10 significant privacy interest groups	Exceeded. 35 meetings were held with or presentations made 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 month of being made available

Achieved.

The internal target for placing new information on the website is within a week, we would normally achieve this within 24 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 they are received.

---

### **Output 3 – Compliance**

Handle complaints of interference with privacy.

Enhance cooperation between privacy regulators internationally.

Undertake Commissioner initiated investigations (as required).

Monitor active information matching programmes.

Quantity	Estimation	Achieved
Number of complaints received	600	806
Number of current complaints processed to completion or settled or discontinued	600	822
Projected number of active information matching programmes monitored	46	46

Quantity	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	<p>Achieved.</p> <p>Survey of both complainants and respondents conducted through 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.</p> <p>72% of complainants rated the complaints process as satisfactory or better. 88% of the respondents rated the complaints process as satisfactory or better. Overall 80% of those who replied felt the process was satisfactory or better.</p>
When a Human Rights Review Tribunal case is concluded the outcome will be reviewed against the work of the office and the findings reported to the Privacy Commissioner	<p>Achieved.</p> <p>The Assistant Commissioner (Legal) reviews and circulates comment and reports as part of monthly reporting to the Privacy Commissioner.</p>
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	<p>Not achieved.</p> <p>External reviewer unable to undertake work prior to 30 June 2009.</p>

---

Referrals to the Director of Proceedings meet expected standards of evidential sufficiency and public interest in all cases

Achieved.  
The Director has expressed strong satisfaction.

---

Reports on authorised information matching programmes to be published will be submitted to relevant departments for comment before publication

Achieved.  
Reports are submitted to relevant departments prior to publication in the annual report.

---

**Timeliness**

**Achievement**

---

80-90% of complaints are completed, settled or discontinued within 12 months of receipt

Exceeded.  
94% of complaints were completed, settled or discontinued within 12 months of receipt.

---

A report on all authorised 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 2009

### 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 2009, and were approved by the Commissioner on 30 October 2009. 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 financial performance 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 financial performance. 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 financial performance 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 financial performance.

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 financial performance 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 financial performance.

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 financial performance.

### **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 financial performance 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 financial performance.

## **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 financial performance, 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 15.

### **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 2009:

#### **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.

### **Standards, amendments and interpretations issued that are not yet effective and have not been early adopted**

Standards, amendments and interpretations issued but not yet effective that have not been early adopted, and which are relevant to the Privacy Commissioner include:

NZ IAS 1 Presentation of Financial Statements (revised 2007) replaces NZ IAS 1 Presentation of Financial Statements (issued 2004) and is effective for reporting periods beginning on or after 1

January 2009. 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 the Crown in its capacity as “owner”. The revised standard gives the Privacy Commissioner the option of presenting items of income and expense and components of other comprehensive income either in a single statement of comprehensive income with subtotals, or in two separate statements (a separate income statement followed by a statement of comprehensive income). The Privacy Commissioner intends to adopt this standard for the year ending 30 June 2010, and is yet to decide whether it will prepare a single statement of comprehensive income or a separate income statement followed by a statement of comprehensive income.

### 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.

## Statement specifying financial performance

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

Specified financial performance	Target \$000	Achievement \$000
Operating Grant	3,148	3,148
Other Revenue	375	552
Total Expenditure	3,523	3,861

### Output Operating Performance

The Privacy Commissioner committed to provide three output classes in 2008/09 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	1,255	1,359
Communications	832	901
Compliance	1,478	1,601
Total	3,565	3,861

## Statement of financial performance

FOR THE YEAR ENDED 30 JUNE 2009

	Note	Actual 2009 \$000	Budget 2009 \$000	Actual 2008 \$000
Crown revenue	2	3,148	3,148	3,109
Other revenue	3	383	315	319
Interest income		69	60	71
<b>Total operating revenue</b>		<b>3,600</b>	<b>3,523</b>	<b>3,499</b>
Marketing		117	72	77
Audit Fees		21	20	26
Depreciation and Amortisation	1, 10, 11	202	168	205
Rental Expense		357	324	369
Operating Expenses	4	532	435	737
Staff Expenses	5	2,620	2,546	2,337
<b>Total Expenses</b>		<b>3,849</b>	<b>3,565</b>	<b>3,751</b>
<b>Net deficit for the period</b>		<b>(249)</b>	<b>(42)</b>	<b>(252)</b>

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

## Statement of changes in equity

FOR THE YEAR ENDED 30 JUNE 2009

	Note	Actual 2009 \$000	Budget 2009 \$000	Actual 2008 \$000
Public equity as at 1 July		875	868	1,127
Net deficit		(249)	(42)	(252)
Total recognised revenues and expenses for the period		(249)	(42)	(252)
<b>Public equity as at 30 June</b>	<b>6</b>	<b>626</b>	<b>826</b>	<b>875</b>

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

## Statement of financial position

AS AT 30 JUNE 2009

	Note	Actual 2009 \$000	Budget 2009 \$000	Actual 2008 \$000
<b>PUBLIC EQUITY</b>				
General funds	6	626	826	875
<b>TOTAL PUBLIC EQUITY</b>		<b>626</b>	<b>826</b>	<b>875</b>
Represented by:				
<b>ASSETS</b>				
<b>Current assets</b>				
Cash and cash equivalents	7	620	662	534
Debtors and other Receivables	8	144	–	173
Prepayments	8	8	8	8
Inventory	9	10	5	4
<b>Total current assets</b>		<b>782</b>	<b>675</b>	<b>719</b>
<b>Non-current assets</b>				
Property, plant and equipment	10	280	332	403
Intangible assets	11	123	132	188
<b>Total non-current assets</b>		<b>403</b>	<b>464</b>	<b>591</b>
<b>Total assets</b>		<b>1,185</b>	<b>1,139</b>	<b>1,310</b>
<b>LIABILITIES</b>				
<b>Current liabilities</b>				
Creditors and other Payables	12	372	255	266
Employee entitlements	13	187	58	170
<b>Total current liabilities</b>		<b>559</b>	<b>313</b>	<b>436</b>
<b>Total liabilities</b>		<b>559</b>	<b>313</b>	<b>436</b>
<b>NET ASSETS</b>		<b>626</b>	<b>836</b>	<b>875</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 2009

	Note	Actual 2009 \$000	Budget 2009 \$000	Actual 2008 \$000
<b>CASH FLOWS FROM OPERATING ACTIVITIES</b>				
Cash was provided from:				
Supply of outputs to the Crown		3,148	3,148	3,109
Revenues from services provided		483	315	300
Interest received		69	60	71
Cash was applied to:				
Payments to suppliers		(952)	(851)	(1,150)
Payments to employees		(2,603)	(2,546)	(2,444)
Net Goods and Services Tax		(46)	25	18
<b>Net cash flows from operating activities</b>	<b>14</b>	<b>99</b>	<b>151</b>	<b>(96)</b>
<b>CASH FLOWS FROM INVESTING ACTIVITIES</b>				
Cash was provided from:				
Cash was applied to:				
Purchase of Property Plant and equipment		(13)	(36)	(259)
Purchase of Intangible Assets		–	–	(83)
<b>Net cash flows from investing activities</b>		<b>(13)</b>	<b>(36)</b>	<b>(342)</b>
Net increase (decrease) in cash held		86	115	(438)
Plus opening cash		534	547	972
<b>Closing cash balance</b>		<b>620</b>	<b>662</b>	<b>534</b>
Cash and bank		620	662	534
<b>Closing cash balance</b>		<b>620</b>	<b>662</b>	<b>534</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 2009

	Actual 2009 \$000	Actual 2008 \$000
Capital commitments approved and contracted		
Non-cancellable operating lease commitments, payable		
Not later than one year	259	325
Later than one year and not later than two years	160	251
Later than two years and not later than five years	334	465
Later than five years	–	–

### 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 2009, the Privacy Commissioner is in the process of renegotiating the lease post December 2009. 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.

A significant portion of the total non-cancellable operating leases. The Privacy Commissioner has assumed she will not vacate the premises at the lease renewal date of August 2010. 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 2009

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 (2008 : nil).

## Notes to the financial statements

FOR THE YEAR ENDED 30 JUNE 2009

### Note 1: Net Deficit for the Period

	Actual 2009 \$000	Actual 2008 \$000
The net deficit is after charging for:		
Fees paid to auditors		
External audit		
Current Year	20	20
Prior Year	1	6
Depreciation:		
Furniture & Fittings	86	84
Computer Equipment	32	26
Office Equipment	19	19
Total Depreciation for the year	137	129
Amortization of Intangibles	65	76
Rental expense on operating leases	356	369

### Major budget variation

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

#### Statement of Financial Performance

##### *Total operating revenue*

Total operating revenue exceeded budget due to additional revenue received from the Ministry of Social Development to facilitate a Code of Practice, treated as other revenue.

##### *Operating expenses*

Operating expenses exceeded budget principally due to increased operating expenditure which was met from reserves held by the Privacy Commissioner. Contributing areas included:

##### *Rent and rates*

Expenses were higher than budget due to unbudgeted increases through the year

### *Marketing*

An additional Privacy Awareness Week to align with an international change was unbudgeted expenditure.

### *Publications*

Production of Guidelines and other educational materials unbudgeted for but met from reserves.

### *Staff expenses*

Increased personnel costs were attributable to the pilot projects of having a Communications Advisor as a fixed term position.

### *Contract services*

Additional contracted services to provide for the completion of the work funded by the Ministry of Social Development.

### *Depreciation*

Higher than budgeted depreciation due to changes associated with the treatment of some assets under NZ IFRS.

## **Statement of Financial Position**

### *Creditors and other payables*

Higher than budgeted due to income in advance received from the Ministry of Health for work to be undertaken in the subsequent year.

### *Employee entitlements*

Employee entitlements are higher than budgeted due in part to higher than expected leave accruals but more significantly in that the budget was set lower than should have been expected.

## **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 (2008: nil).

### Note 3: Other revenue

	Actual 2009 \$000	Actual 2008 \$000
Other grants received	236	116
Rental income from property sub-leases	23	31
Privacy Forum	39	2
Seminars & workshops	56	66
Other	29	104
<b>Total other revenue</b>	<b>383</b>	<b>319</b>

### Note 4: Operating expenses

	Actual 2009 \$000	Actual 2008 \$000
Website development expenses	33	42
Inventories consumed	19	2
<b>Other expenses</b>	<b>52</b>	<b>44</b>

### Note 5: Staff expenses

	Actual 2009 \$000	Actual 2008 \$000
Salaries and wages	2,410	2,220
Employer contributions to defined contribution plans	32	32
Other staff expenses	28	21
Increase in employee entitlements (note 13)	17	64
Other contracted services	133	–
<b>Total staff expenses</b>	<b>2,620</b>	<b>2,337</b>

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

## Note 6: General funds

	Actual 2009 \$000	Actual 2008 \$000
Opening balance	875	1,127
Net deficit	(249)	(252)
<b>Closing balance</b>	<b>626</b>	<b>875</b>

## Note 7: Cash and cash equivalents

	Actual 2009 \$000	Actual 2008 \$000
Cash on hand and at bank	270	108
Cash equivalents – term deposits	350	426
<b>Total cash and cash equivalents</b>	<b>620</b>	<b>534</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 2009 \$000	Actual 2008 \$000
Trade debtors	144	173
Prepayments	8	8
<b>Total</b>	<b>152</b>	<b>181</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 (2008 \$NIL).

As at 30 June 2009 and 2008, 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 2009 no debtors have been identified as insolvent (2008 \$NIL).

## Note 9: Inventories

	Actual 2009 \$000	Actual 2008 \$000
Publications held for sale	10	4

The carrying amount of inventories held for distribution that are measured at current replacement cost as at 30 June 2009 amounted to \$NIL (2008 \$NIL).

There have been no write-down of inventories held for distribution or reversals of write-downs (2008 \$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 2007	274	100	109	483
Additions	207	46	5	258
Balance at 30 June 2008	481	146	114	741
Balance at 1 July 2008	481	146	114	741
Additions	–	13	–	13
Balance at 30 June 2009	481	146	114	754
<b>ACCUMULATED DEPRECIATION AND IMPAIRMENT LOSSES</b>				
Balance at 1 July 2007	107	45	56	208
Depreciation expense	84	26	19	129
Balance at 30 June 2008	191	71	75	337
Balance at 1 July 2008	191	71	75	337
Depreciation expense	86	33	19	138
Balance at 30 June 2009	277	104	94	475
<b>CARRYING AMOUNTS</b>				
At 1 July 2007	120	67	57	244
At 30 June and 1 July 2008	290	75	39	404
At 30 June 2009	204	55	20	279

## Note 11: Intangible assets

Movements for each class of intangible asset are as follows:

	Acquired software \$000
<b>COST</b>	
Balance at 1 July 2007	210
Additions	84
Balance at 30 June 2008	294
Balance at 1 July 2008	294
Additions	–
Balance at 30 June 2009	294
<b>ACCUMULATED AMORTISATION AND IMPAIRMENT LOSSES</b>	
Balance at 1 July 2007	30
Amortisation expense	76
Balance at 30 June 2008	106
Balance at 1 July 2008	106
Amortisation expense	65
Balance at 30 June 2009	171
<b>CARRYING AMOUNTS</b>	
At 1 July 2007	–
At 30 June and 1 July 2008	180
<b>At 30 June 2009</b>	<b>123</b>

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 2009 \$000	Actual 2008 \$000
Creditors	69	67
Income in advance	120	–
Accrued expenses	93	36
Other payables	90	163
<b>Total creditors and other payables</b>	<b>372</b>	<b>266</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 2009 \$000	Actual 2008 \$000
Current employee entitlements are represented by:		
Accrued salaries and wages	61	51
Annual leave	126	119
<b>Total current portion</b>	<b>187</b>	<b>170</b>
Current	187	170
Non-current	–	–

**Note 14: Reconciliation of the net surplus from operations with the net cashflows from operating activities**

	Actual 2009 \$000	Actual 2008 \$000
Net deficit from operations	(249)	252
Add (less) non-cash items:		
Depreciation and amortisation	202	205
Other non cash items	202	–
<b>Total non-cash items</b>	<b>205</b>	<b>205</b>
Add (less) movements in working capital items:		
Increase in receivables	30	(117)
(Increase)/Decrease in prepayments	–	99
(Increase)/Decrease in inventory	(6)	1
Decrease in payables	(15)	(96)
Increase in employee entitlements	17	64
Increase in income advance	120	–
<b>Working capital movements – net</b>	<b>146</b>	<b>(49)</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>99</b>	<b>(96)</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. In the 2008-09 year the Office made payment to the Trust of \$200 being membership fees for the year. The transaction was undertaken around normal business terms.

The Privacy Commissioner received \$2,000 in sponsorship to co-host Privacy Awareness Week in May 2009. The sponsorship was provided by Symantec Australia Limited, the funds were provided in accordance with the Office Sponsorship and Partnership Policy.

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 2009 \$000	Actual 2008 \$000
Total salaries and other short-term employee benefits	832	660

Key management personnel include all Senior Management Team members, the Privacy Commissioner who together comprise the Leadership Team. The General Manager joined the Senior Management Team in the 2008-09 year.

### 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 2009 \$000	Actual 2008 \$000
\$100,000 – \$110,000		
\$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	

### Note 17: Commissioner's 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 2008 to 30 June 2009.

Name	Position	Amount 2009	Amount 2008
Marie Shroff	Privacy Commissioner	\$263,502	\$246,359

### Note 18: Cessation payments

No redundancy payments were made in the year.

### 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**

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 2009 (2008: 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 Commissioners 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>2009</b>				
Financial assets				
Cash and cash equivalents	5.88	6.20	–	–
	<b>5.88</b>	<b>6.20</b>	<b>–</b>	<b>–</b>
<b>2008</b>				
Financial assets				
Cash and cash equivalents	8.27	534	–	–
	<b>8.27</b>	<b>534</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 2009 NZ\$000	Net surplus 2008 NZ\$000
Cash and cash equivalents +100 bps	6.2	5.34
Cash and cash equivalents -100 bps	(6.2)	(5.34)

Privacy's sensitivity to interest rate changes has not changed significantly from the prior year.











