

Privacy Commissioner

Annual Report 2011



Privacy Commissioner
Te Mana Matapono Matatapu



Privacy Commissioner
Te Mana Matapono Matatapu

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

© 2011 The Privacy Commissioner

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

ANNUAL REPORT OF THE PRIVACY COMMISSIONER


For the year ended 30 June 2011

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

November 2011

THE MINISTER OF JUSTICE

I tender my report as Privacy Commissioner
for the year ended 30 June 2011.

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

Marie Shroff
Privacy Commissioner

CONTENTS

1: KEY POINTS	9
2: INTRODUCTION	13
3. REPORT ON ACTIVITIES	17
International activities	17
Highlights	18
Information services	18
Enquiries	18
Training and education	19
Privacy Awareness Week	19
Your privacy – but is it really yours? The youth privacy project	20
Senior citizens' focus group	21
Reviewing and improving our website: privacy.org.nz	21
Other outreach	21
Media	22
Complaints and access reviews	22
The complaints process	23
Overview of 2010/11	24
Settlement	25
Personal contact	26
Complaints received	26
Agency types	27
Age of complaints	27
Complaint outcomes	28
Top respondent agencies	28
Satisfaction survey	30
External audit	30
Litigation	31
Human Rights Review Tribunal	31
Judicial review	32
Employment Court	33
Commissioner initiated inquiries	33
Google WiFi	33
Access to Telecom customer information by competitor	34
Audio-recording in taxis	34
Section 54 authorisations	34
Policy	35
Legislation	37

CONTENTS

Health advice	37
Technology advice	37
Law Commission's review of privacy	38
Information matching	39
Codes of practice	39
Credit Reporting Privacy Code	39
Christchurch Earthquake (Information Sharing) Code 2011 (Temporary)	40
Consultations with the Ombudsmen	42
4: OFFICE OF THE PRIVACY COMMISSIONER	45
Independence and competing interests	45
Reporting	45
Staff	45
Equal employment opportunities	46
5. INFORMATION MATCHING	49
Information matching and privacy – an introduction	49
Glossary	51
The year in information matching	52
Highlighted errors	52
Outreach	53
Changes in authorised and operating programmes	53
Periodic review (s.106) of information matching programmes	54
Online transfer approvals	54
Programme Reports	56
1. Corrections/ACC Prisoners Programme	57
2. IR/ACC Levies and Compensation Programme	57
3. Citizenship/BDM Citizenship by Birth Processing Programme	58
4. BDM/DIA(C) Citizenship Application Processing Programme	59
5. BDM/DIA(P) Passport Eligibility Programme	59
6. Citizenship/DIA(P) Passport Eligibility Programme	60
7. NZTA/EEC Unenrolled Voters Programme	61
8. MoT/EEC Unenrolled Voters Programme	61
9. MSD/EEC Unenrolled Voters Programme	62
10. Citizenship/EEC Unenrolled Voters Programme	63
11. INZ/EEC Unqualified Voters Programme	63
12. BDM(Deaths)/GSF Eligibility Programme	64
13. BDM (Deaths)/INZ Deceased Temporary Visa Holders Programme	65
14. Citizenship/INZ Entitlement to Reside Programme	65

CONTENTS

15. Corrections/INZ Prisoners Programme	66
16. Customs/IR Child Support Alerts Programme	67
17. Customs/IR Student Loan Interest Programme	68
18. MSD/IR Working For Families Tax Credits Administration Programme	69
19. MSD/IR Working for Families Tax Credits Double Payment Programme	69
20. Customs/Justice Fines Defaulters Alerts Programme	70
21. INZ/Justice Fines Defaulters Tracing Programme	71
22. IR/Justice Fines Defaulters Tracing Programme	72
23. MSD/Justice Fines Defaulters Tracing Programme	73
24. BDM (Births)/Ministry of Health NHI and Mortality Register Programme	74
25. BDM (Deaths)/Ministry of Health NHI and Mortality Register Programme	74
26. ACC/MSD Benefit Eligibility Programme	75
27. BDM/MSD Identity Verification Programme	76
28. BDM (Deaths)/MSD Deceased Persons Programme	78
29. BDM (Marriages)/MSD Married Persons Programme	78
30. Centrelink/MSD Change in Circumstances Programme	79
31. Centrelink/MSD Periods of Residence Programme	80
32. Corrections/MSD Prisoners Programme	80
33. Customs/MSD Arrivals and Departures Programme	81
34. Customs/MSD Periods of Residence Programme	82
35. Educational Institutions/MSD (StudyLink) Loans and Allowances Programme	82
36. HNZ/MSD Benefit Eligibility Programme	83
37. IR/MSD Commencement/Cessation Benefits Programme	84
38. IRD/MSD Commencement/Cessation Students Programme	86
39. IR/MSD Community Services Card Programme	87
40. IR/MSD Debtors Tracing Programme	87
41. IR/MSD (Netherlands) Tax Information Programme	88
42. Ministry of Education/MSD (StudyLink) Results of Study Programme	89
43. Netherlands/MSD Change in Circumstances Programme	90
44. Netherlands/MSD General Adjustment Programme	90
45. BDM (Deaths)/NPF Eligibility Programme	91
46. BDM (Deaths)/NZTA Deceased Driver Licence Holders Programme	92
47. MoE/Teachers Council Registration Programme	92
6: Financial & Performance Statements	95
Statement of responsibility	95
Audit Report	96

CONTENTS

Statement of objectives and service performance 2010/11	98
Statement of accounting policies for the year ended 30 June 2011	105
Statement specifying comprehensive income	114
Statement of comprehensive income for the year ended 30 June 2011	115
Statement of changes in equity for the year ended 30 June 2011	115
Statement of financial position as at 30 June 2011	116
Statement of cash flows for the year ended 30 June 2011	117
Statement of commitments as at 30 June 2011	118
Statement of contingent liabilities as at 30 June 2011	118
Notes to the financial statements for the year ended 30 June 2011	119

Section 3 Tables

Table 1: Complaints received and closed 2006-2011	23
Table 2: Settlement outcomes 2010/11	26
Table 3: Act/Code – breakdown of complaints received 2010/11	26
Table 4: Complaints received by agency type 2010/11	27
Table 5: Outcomes on closed files 2010/11	28
Table 6: Complaints received and closed for top respondent agencies 2010/11	29
Table 7: Outcomes for top respondent agencies 2010/11	29
Table 8: Referrals, tribunal cases and outcomes 2005-2011	31

Section 4 Tables

Table 9: Office of the Privacy Commissioner workplace gender profile 2010/11	46
Table 10: Office of the Privacy Commissioner workplace ethnic profile 2010/11	47

Section 5 Tables

Table 11: First time approvals 2010/11	55
Table 12: Renewed approvals 2010/11	55

Figures

Figure 1: Outcomes on complaints 2010/11	24
Figure 2: Age of closed complaints 2010/11	27
Figure 3: Active authorised information matching programmes 2010/11	52
Figure 4: Authorised, operating and inoperative information matching programmes 2002-2011	54

1: KEY POINTS

1: KEY POINTS

Information and communications

- We received just over 7,000 enquiries from members of the public and organisations seeking advice on privacy matters.
- This year we had 212 media enquiries. About 80 percent of these enquiries were driven by external events, incidents or developments, such as location based technology, Facebook practices or loss of client information by businesses.
- This year's Privacy Awareness Week, run with our partners from the Asia Pacific Privacy Authorities (APPA) forum, featured an international online survey about social media, which got over 10,000 responses. We will release the results later in 2011.
- We finalised our new education kit for schools, "Your privacy – but is it really yours?", and distributed it to secondary schools and organisations working with youth.
- We released our health information toolkit, containing fact sheets, a narrated PowerPoint presentation, a new edition of "On the Record" and health case notes.
- We formed an advisory group of senior citizens to listen to what they had to say about privacy. They helped us to develop advice on the five topics that they saw as most important: financial privacy, scams, health information, business use of information, and keeping safe online.
- The Office delivered 37 workshops and seminars to members of the public and stakeholder groups. The Commissioner and staff also gave 44 presentations, such as to health and business groups, both in New Zealand and overseas.

Investigations

- We received 968 complaints, a similar number to last year.
- 28 percent of complaints were closed by settlement or mediation, an increase from last year. We try to move parties towards settlement, helping them to avoid the expense and stress of tribunal proceedings.
- 96 percent of complaints are under 12 months of age, with 80 percent closed within six months of receipt.

Policy and technology

- We monitored 47 active government information matching programmes this year, 31 of which use online data transfers.
- Policy work during the year involved a wide range of projects with central and local government, the private sector, industry bodies and voluntary organisations. We advised on major legislative projects including the Search and Surveillance Bill, the Customs and Excise (Joint Border Management and Information Sharing) Bill, the Taxation (Tax Administration and Remedial Matters) Bill and the Courts and Criminal Matters Bill.
- Amendment No.4 to the Credit Reporting Privacy Code 2004 was issued in December 2010. This took the first steps towards allowing greater collection of personal information, balanced with more stringent safeguards such as providing a credit freezing facility and information to the public about their rights. We put out a consultation draft of Amendment No.5 at the end of May 2011, which moves further towards a more comprehensive credit reporting system.
- We continued to work with the Law Commission on its review of the Privacy Act. We supported the Law Commission's development of recommendations that would upgrade our 18 year old Privacy Act and provide some additional tools to protect New Zealanders' personal information in the digital age.
- We conducted a survey of major public and private sector organisations about their use of offshore information and communications technologies, including cloud computing services. We are using the survey results to work towards guidance on how to manage privacy as part of cloud computing.
- We developed "Getting Started" (privacy.org.nz/getting-started), a tool to help agencies think about how to get privacy right when they are developing policy projects.
- We issued the Christchurch Earthquake (Information Sharing) Code 2011 (Temporary) to enable those dealing with the emergency to share personal information to assist victims of the earthquake and their families, and to help in the coordination and management of the response.

International

- We made substantial progress in securing a finding from the EU that New Zealand offers an 'adequate standard of data protection'. In February, New Zealand's law received a positive recommendation from the influential Article 29 Working Party.
- We hosted the annual Asia Pacific Privacy Authorities Forum in Auckland in December, bringing together delegates from as far afield as Mexico and Macau.
- The Office assisted in the establishment of the Global Privacy Enforcement Network (GPEN) and became a founding member when it started in September.

2: INTRODUCTION

2: INTRODUCTION

Some headlines from our year

Equipping the Privacy Commissioner for the 21st century

We worked with the Law Commission during the year on its review of the Privacy Act. The Commission's package of recommendations will help to power up privacy law for the 21st century.

In particular, the Law Commission has recognised that we need some additional legal tools to be effective, particularly in the digital age. There are a growing number of issues that cannot be properly addressed through a complaints system alone. People cannot complain if they do not realise what is happening with their information – and, increasingly, government and business practices fly below people's radar. Also, a complaints system can only be driven by problems after they occur. It is becoming more and more important to find out what is happening before things go wrong.

So, for example, the Law Commission has suggested we should be able to order agencies to comply with the law and to release information to requesters, and that we should be able to audit or to order agencies to self-audit their systems. We think these are tools that would streamline how we can deal with the issues that are of most importance for New Zealanders' privacy. Mandatory notification of privacy breaches would help people to protect themselves when things go wrong, as well as bringing careless companies to heel. And a statutory "do not call" scheme would give people greater choices over whether their information is used for marketing.

We look forward to seeing the Government's response in early 2012 to the Law Commission's recommendations.

Another year, another set of technology challenges

As usual, we have kept a close eye on developments in the field of information and communications technology ("ICT") during the year.

We released a survey in May on how agencies make international disclosures and use offshore ICT: <http://privacy.org.nz/assets/Files/Media-Releases/Overseas-ICT-Survey.pdf>. Fifty major public and private sector organisations answered the survey, most of whom hold large amounts of personal information. We are using the survey results to work towards guidance on how to manage privacy as part of cloud computing.

We also conducted a survey on social networking, together with our partners in the Asia Pacific Privacy Authorities forum. The results will be released in December.

Security challenges and new privacy questions continue to raise their heads, even for big ICT firms. For example, this year saw Sony repeatedly become the target of hackers. Apple and Google were called before Senate committees in the United States to explain how their products use geolocation features. Facebook and LinkedIn fielded questions from their users (as well as regulators) about unilateral changes to their privacy settings. And web services that require users to use their real name are sparking debate over when it is acceptable for people to transact anonymously or pseudonymously, both online and offline.

The News of the World phone accessing scandal led to serious questions being asked in several jurisdictions about media behaviour – and about people's own awareness of how to secure their private communications. It also raised issues about how to deal with “blagging” (impersonation of others to get information).

Managing identity continues to be a field of significant interest, particularly for government and major businesses. For instance, we have close contact with the New Zealand i-government initiative. The new regulations to combat money laundering also involve the need for businesses to be certain that people are who they say they are. And biometric technologies continue to get more reliable, more ubiquitous, and smarter.

Data collection, data mining and data regulation – getting the balance right

It is a common saying that ‘information is power’ but, these days, it is probably even more correct to say that ‘information is money’. Many of the current challenges to privacy arise because of the cash value that personal information has.

This is not to say that making a profit from personal information is necessarily bad. On the contrary, many legitimate businesses (including credit reporters, online service providers and targeted marketing enterprises) play a major part in our economy and in the way our society operates. However, it is increasingly important for all those businesses to get privacy right in everything they do. As the regulator in the area, we have to play a major part in making sure that the benefits of information collection and use are balanced with proper respect for the people behind the information.

We have nearly completed work on possible reforms to the Credit Reporting Privacy Code. We issued a consultation draft in May and held public hearings about the possibility of permitting more comprehensive information to be stored and used on credit reports.

The changes to the Code would include more stringent safeguards such as providing a credit freezing facility and better information to the public. By the time this Annual Report is published, we will have issued the Code amendments.

Parliament has also passed a law (the Courts and Criminal Matters Bill) permitting outstanding court fines to be added to credit reports. This will also add to the variety of information available on credit reports.

Collection of information into large databases was also highlighted this year when New Zealand Post conducted its second Lifestyle Survey, inviting people to complete a detailed questionnaire in exchange for a chance to win a prize. The information that people submitted was added to a database, and mined to produce lists that businesses with particular marketing niches could rent. This is only one of an increasing number of examples of collection and use of "big data" by business and government – this is an area that we will be paying close attention to in the years to come.

Changing how government agencies share information

A major aspect of the Law Commission's review of the Privacy Act was to recommend a new method by which government agencies could share personal information.

Instead of having to pass primary legislation if agencies wish to share information in a way that might breach the privacy principles, the recommendation is that an Order in Council can approve information sharing agreements between government agencies.

The recommendation is finely balanced to try to make sure that conditions for public trust in government and privacy are maintained, as well as making sure that justified information sharing can be done efficiently. It includes major safeguards including full consultation with my Office before an agreement can go to Cabinet, the ability for me to publish reports with my view about an agreement, the ability for agreements to be disallowed, and also for them to be regularly reviewed.

3. REPORT ON ACTIVITIES

3. REPORT ON ACTIVITIES

International activities

There is an international dimension to many aspects of information privacy and protection. Most significant is the cross-border transfer of personal information that is so much an ordinary daily feature of business and personal life today. In addition to changes in business process, such as outsourcing and off-shoring, individuals are publishers of content and not merely consumers of it. It is now a routine matter for individuals to publish personal information about themselves and others literally to the world – something that would have been beyond the technical capability of most New Zealanders a decade ago.

The Office engages at the international level in a number of ways and for various purposes. For example:

- It is important to develop common norms and standards where possible. Compatible approaches in different countries are essential to facilitate business transactions and to protect individuals.
- A company's actions in one country can easily affect the citizens in another. For instance the company may develop policies that apply across the world or may experience a security breach involving customers in several jurisdictions.
- We may need to seek the cooperation of companies based overseas or to ask regulators and enforcement authorities in other countries to investigate a privacy breach that a New Zealander has experienced with a company outside our jurisdiction.
- Other countries frequently encounter privacy challenges before New Zealand does. Collaboration with overseas counterpart authorities can lead to enhanced problem solving, creative policy solutions and more effective regulation.

The Office engages in a variety of international forums. The principal ones are:

- *Asia Pacific Privacy Authorities (APPA) Forum*: meets twice a year and involves commissioners from Australia, Canada, Hong Kong, Korea, Mexico, New Zealand and the USA.
- *International Conference of Data Protection and Privacy Commissioners*: brings together more than 90 Privacy Commissioners from around the world in an international conference and also involves inter-sessional work through several working groups.

- *APEC*: the Data Privacy Sub-group (DPS) is APEC's specialist group devoted to privacy policy issues, while the Cross-border Privacy Enforcement Arrangement (CPEA) is a network of participating privacy enforcement authorities.
- *OECD*: the Working Party on Information Security and Privacy (WPISP) brings together privacy expertise across OECD countries to advance policy objectives.

Highlights

Some of the highlights during 2010/11 were:

- *OECD*: The Office continued its contribution to the OECD Review of the 1980 Privacy Guidelines, including a presentation by the Privacy Commissioner to an OECD conference in October. We facilitated the preparation of a consolidated civil society response to an OECD questionnaire on the review in March.
- *European Union*: The Office made further progress in securing a finding from the EU that New Zealand offers an 'adequate standard of data protection' including obtaining, in February, a positive recommendation from the influential Article 29 Working Party.
- *Asia Pacific Privacy Authorities Forum*: In December, we successfully hosted an APPA meeting in Auckland bringing together delegates from as far afield as Mexico and Macau.
- *Global Privacy Enforcement Network*: We assisted in the establishment of GPEN, became a founding member when it commenced in September, and joined the inaugural GPEN Participation Committee.
- *APEC Cross-border Privacy Enforcement Arrangement*: we assisted in the launch of CPEA in July 2010 and became a CPEA co-Administrator.
- *International Conference of Data Protection and Privacy Commissioners*: The Privacy Commissioner participated in the 32nd Annual Conference and was re-elected as convenor of the steering group on representation before international organisations.

Information services

Enquiries

We received just over 7,000 individual contacts through our enquiries services – a similar number to last year.

The service operates an 0800 phone line and an email address. About 80 percent of the enquiries were received by telephone. Email contact is increasing and comprised 17 percent of enquiries.

Approximately one third of all enquiries were about the disclosure of personal information, nearly a third of enquiries were about collection issues, with the next biggest area of enquiry about access issues. Combined, these three areas made up about 80 percent of enquiries.

By far the largest group of callers were individuals seeking advice. The next largest group were health sector organisations.

Despite the seriousness of the Canterbury earthquakes, we received only a modest number of calls for assistance. In the immediate aftermath of the quakes, most calls were about access to and disclosure of information that would assist with the rescue activities. Later in the year, the enquiries involved access to information about insurance activities and assessment of damage.

The New Zealand Post Lifestyle Survey also resulted in more than 30 calls. Generally, these raised concerns about the appropriateness of the survey.

Training and education

This was a quieter year for our education work. Seven of our regular workshops were cancelled due to lack of sufficient numbers. The fees we charge as cost-recovery for the workshops have remained the same for some time now, and the feedback we receive about the workshops continues to say they are relevant and useful. The reason for the lack of numbers therefore appears to be linked to the financial downturn and to increased pressure on budgets in both the public and private sectors.

However, we still conducted 37 workshops and seminars. These were generally run by our investigations staff, with some provided by contractors. As in previous years, there was a high demand for education within the health sector.

Courses were delivered in Auckland, Hamilton, New Plymouth, Wairarapa, Palmerston North, Wellington, Nelson and Christchurch.

Privacy Awareness Week

Privacy Awareness Week is an international event run by the Asia-Pacific Privacy Authorities forum ("APPA"). It is held in the first week in May and involves New Zealand, most Australian jurisdictions, Hong Kong, South Korea, Canada and – for the first time in 2012 – the United States and Mexico.

This year, APPA put together an online social media survey which got just over 10,000 responses. More than 1,200 people responded from New Zealand. This was an excellent rate of return for a small jurisdiction. We particularly valued the assistance of Trade Me, which provided free advertising space for the APPA survey during Privacy Awareness Week, with a facility for people to click through to the survey itself.

The social media survey results will be released later in 2011.

APPA also produced a short, humorous animation showing the privacy pitfalls of social media: <http://privacyawarenessweek.org/video.html>

We did not run a major event in New Zealand for Privacy Awareness Week this year. Instead, we focused our efforts on two key pieces of work:

- We conducted a survey of major public and private sector organisations about their use of offshore information and communications technologies, including cloud computing services. Fifty organisations responded. The survey report is available at: <http://privacy.org.nz/assets/Files/Media-Releases/Overseas-ICT-Survey.pdf>
- We released our health information toolkit, containing plain English fact sheets, a narrated PowerPoint presentation for trainers or privacy officers to use in their own organisations, a new edition of our popular publication “On the Record”, and a variety of health case notes. <http://privacy.org.nz/health-privacy-toolkit/>

The International Association of Privacy Professionals held a seminar in Auckland, featuring the Privacy Commissioner and Google's privacy lead, Alma Whitten. The seminar discussed issues raised by the offshore ICT survey and by the cloud computing environment.

Privacy Awareness Week does not only involve activities by privacy regulators. Instead, it is increasingly becoming a useful date on the calendar for other organisations in New Zealand, both in the public sector and the private sector. These organisations use the week as an opportunity to highlight privacy as it relates to their own business, or to produce new training material.

Your privacy – but is it really yours? The youth privacy project

We reported last year that we had run a focus group of secondary school students to decide what information young people need about privacy, and how best to deliver that information. The result was our youth privacy kit, which we launched in August at Mana College, Porirua.

The youth group called the campaign “Your privacy – but is it really yours?” They wrote a wallet-sized brochure with tips for students on various privacy topics, produced a poster and scripted and filmed a short video. The kit is intended for use in schools and also includes resources for teachers, discussion ideas and guidelines for presenters at events like school assemblies. (<http://privacy.org.nz/youth/>)

We have distributed 111 copies of the kit on request to secondary schools and organisations working with youth.

Senior citizens' focus group

In April, in partnership with the Office for Senior Citizens, we ran a focus group for senior citizens and those working in community organisations for older people.

Like our youth group, this seniors' focus group told us what privacy issues were important to them. The five topics they selected were financial privacy, scams, health information, business use of information, and keeping safe online. They also told us what methods would be effective to deliver that information.

The resulting advice material was launched in late September 2011 and we will report on it next year.

Reviewing and improving our website: privacy.org.nz

We reviewed our website this year, and we have made some changes to improve how the site functions and how people can navigate through it.

Our changes include adding an advanced search function, to improve users' ability to locate information quickly and accurately. Feedback indicates this is working well.

We have also added an auto-subscribe function for our newsletter, other regular publications such as case notes, and our technology and privacy forums. This feature, combined with the existing RSS feed service for items such as our media releases, allows users to automatically receive information without having to visit our website. It is also easy for them to unsubscribe, if they want to. Numbers of subscribers have risen considerably since we introduced this feature.

We are continually checking the site to make changes to assist users. This includes rewriting material to be in plain English, reducing the number of pdfs and enhancing accessibility for people with disabilities.

Other outreach

The Commissioner and her senior staff have given 44 speeches and presentations during the year on a wide range of topics and for a wide variety of audiences. Topics have included:

- Reforming credit reporting law
- Privacy: personal, social and political
- Privacy and technology – innovative partners
- Privacy in the context of the internet – recording everything and forgetting nothing?
- The globe and the cloud – where is the Privacy Commissioner heading?

- Privacy and language interpretation
- Privacy and the media.

Media

In 2008/09 we received 217 media enquiries, followed by an upswing to 323 enquiries in the 2009/10 financial year. This year we reverted to a more normal 212 enquiries.

The majority of enquiries (about 80 percent) arose when journalists contacted us on their own initiative, seeking our response to events, incidents or developments, such as location based technology, Facebook practices or data breaches.

About 20 percent of the enquiries received stemmed from our own publicity (information about Commissioner-initiated inquiries, public statements on topics, or publication of guidance material). Topics included our inquiry into Google's Wi-Fi data collection, the amendments to the credit reporting privacy code and the youth information material.

The shift towards technology-related subjects has continued. Almost all of the enquiries from media arose from developments in technology, and particularly from the way data is collected. Examples included enquiries about body-scanners at airports, geo-location tracking and Facebook applications. Data security breaches also generated much media interest, particularly for high-profile incidents such as the Sony Playstation hacking incidents, but also numerous smaller cases.

The rapidly changing technology landscape is beginning to be reflected by regulatory changes. Our work on offshore ICT and cloud computing practices attracted media interest, as did legislative proposals to better protect New Zealanders' data when it is sent offshore.

Responding to media requests for comment or background information can be challenging for a small office like ours with no full time communications staff. This is particularly where the deadline for comment is short or where an answer requires detailed technical knowledge about an emerging development. However, we believe that responding to media enquiries is an important channel for raising public awareness about privacy risks and protections.

Complaints and access reviews

We received a total of 968 complaints in the 2010/11 year. Table 1 shows incoming and closed complaints and work in progress at year's end. Work in progress at the end of the year was better than our expectations (of between 250 and 350 files).

TABLE 1: COMPLAINTS RECEIVED AND CLOSED 2006-2011

	2006/07	2007/08	2008/09	2009/10	2010/11
Complaints received	640	662	806	978	968
Complaints closed	701	767	822	961	999
Work in progress after year's end	394	289	273	290	247

The complaints process

When we receive a complaint, we assess it on its facts and against the law. Key in this assessment is to analyse whether the complaint is within our jurisdiction, what privacy principles are involved and whether there might be an interference with privacy. We also see whether agencies have breached proper procedure, such as an agency not dealing with an access request within the statutory time frame. And we watch for possible systemic difficulties with information handling in agencies.

For a complaint to be upheld under the Act there has to be an "interference" with the privacy of the complainant. To prove an "interference", a complainant must show a breach of the Act or Codes and that they suffered some harm – either financial loss, loss of a benefit, significant humiliation or embarrassment, or by being wrongly denied access to information they were entitled to receive (or correction of information they wanted to be corrected).

Complaints often ultimately fail because a complainant is unable to show either a breach or harm. But most complaints need to be investigated before we can assess whether the complaint involves an interference with privacy. For instance, we will need to hear the respondent's view.

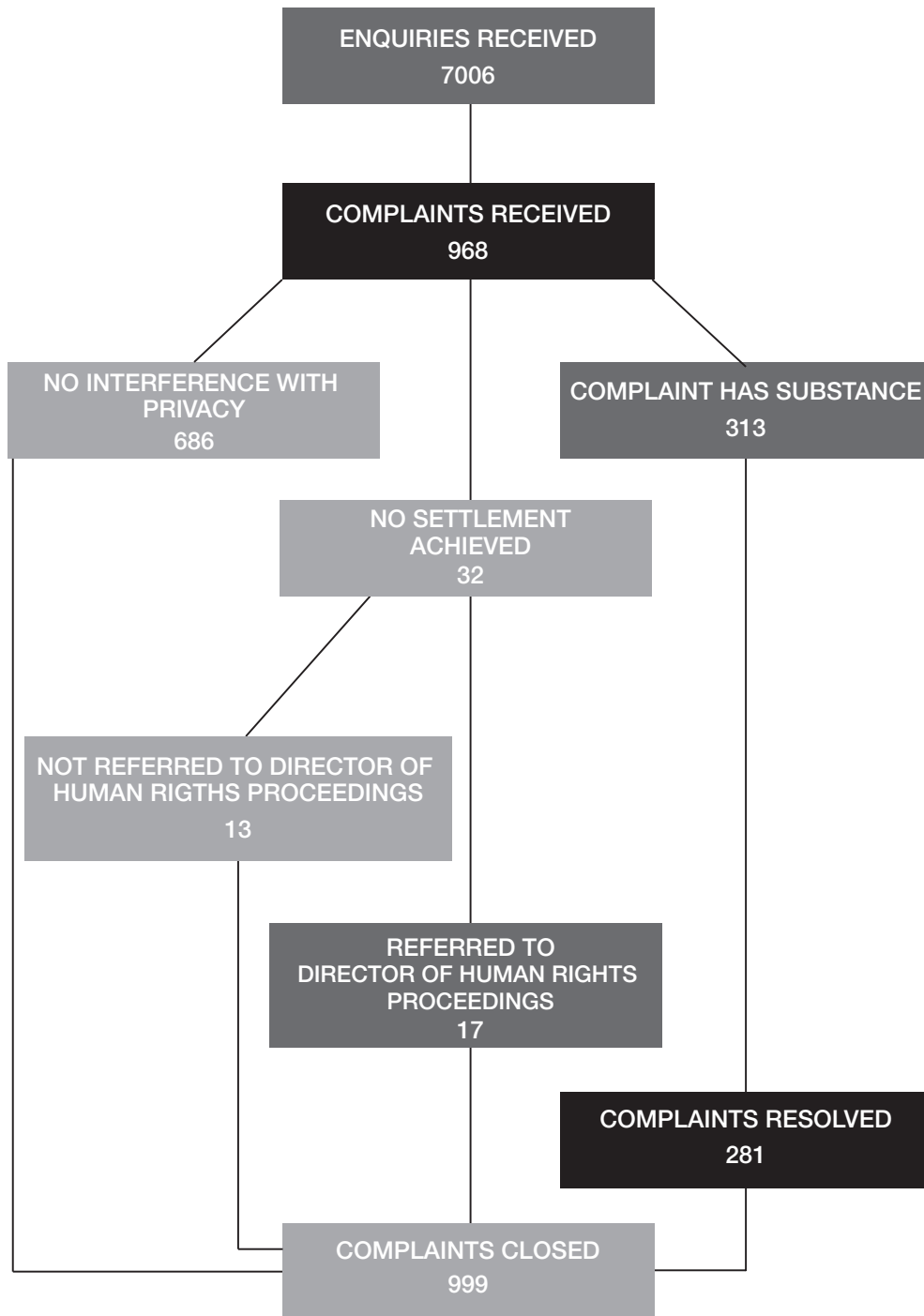
While many complainants have difficulty showing sufficient evidence of harm, some complaints may still be resolved, for example, by the respondent agency providing assurances that they will change their practices or apologising for the circumstances that resulted in the dispute. This is often all the complainant wants.

Many access complaints settle because the respondent agency accepts our view that more information should have been released, and then releases the information.

Where we believe an interference with privacy has occurred, we encourage both parties towards a resolution.

Overview of 2010/11

Figure 1: Outcomes on complaints and enquiries 2010/11



In 2010/11, we closed 686 complaints because our view was that there was no interference with privacy. This was for a variety of reasons including that there was no breach of the Act or that there was no demonstrable harm. In many cases, we found that the agency complained about had adhered to the Act's principles.

In 164 of the 534 access complaints (about 30 percent), our view was that the respondent agencies correctly applied the withholding grounds in sections 27 to 20 of the Act.

In other cases, complainants failed to progress their complaints by either not communicating further with us after they first complained, or by not being able to supply sufficient evidence to support their complaints.

Some complaints were not advanced because other more appropriate remedies were available to the complainant. Examples included going to the Medical Council or taking court action. In some cases, the complaint issue occurred many years ago making it impracticable or undesirable to conduct an investigation. A few complaints were transferred to other complaints agencies that were better able to deal with the issues, such as the Ombudsmen's Office or the Health and Disability Commissioner.

There were 313 complaints that had some substance in one or more of the issues raised in the complaint.

Settlement

Our aim is to settle 30 percent of all complaints. Settlement outcomes for this year are shown in Table 2, below. Of the complaints closed, 28 percent were closed with some type of settlement, which was an increase on our settlement rate from last year.

We achieved some level of resolution in 90% of the complaints that had substance.

281 of the complaints that had some substance (last year, 244) were settled in a variety of ways ranging from an apology accompanied by small gifts and in some cases monetary compensation. This year, monetary compensation was generally for amounts less than \$5,000 with some greater than \$10,000. The highest settlement figure was \$50,000. Some complaints had multiple settlement outcomes such as an apology, assurances and a monetary payment.

TABLE 2: SETTLEMENT OUTCOMES 2010/11

Settlement outcome	Number
Information released	138
Apology	63
Money/monies worth	46
Information partly released	45
Information corrected	18
Assurances	16
Change of policy	14
Generally satisfied	11
Training	1

Personal contact

We continue to believe that conversations with complainants and respondents and direct early contact with both parties increases the potential for settlements. Early personal contact also increases our overall efficiency and reduces the time taken to investigate complaints.

This year we achieved personal contact with one or more of the parties to a complaint on 90 percent (899) of the complaint files.

Complaints received

Past trends continue to be reflected in the incoming complaints for the year. Of the 968 complaints received, more than 75 percent alleged breaches of privacy under the Act's information privacy principles. Table 3 shows a breakdown between the privacy principles and rules contained in the three codes.

TABLE 3: ACT/CODE – BREAKDOWN OF COMPLAINTS RECEIVED 2010/11 (previous year in brackets)

Information Privacy Principle	759	(734)
Health Information Privacy Code	185	(198)
Telecommunications Privacy Code	11	(11)
Credit Reporting Code	6	(6)
Not identified in category	7	(29)
TOTAL	968	(978)

Agency types

Table 4 provides a breakdown of complaints in various sectors. The three major categories occupy over 60 percent of our complaints, with complaints about the public sector being the biggest overall segment.

TABLE 4: COMPLAINTS RECEIVED BY AGENCY TYPE 2010/11
(previous year in brackets)

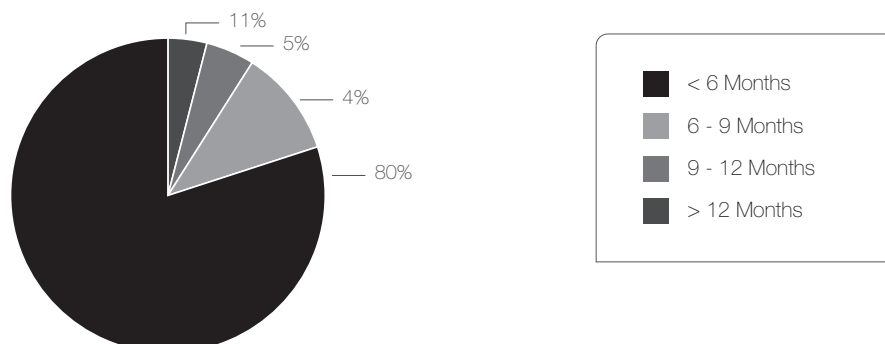
Agency Type	Total	Percentage
Government sector, including education and local authorities	437 (425)	45% (44)
Health sector, including hospitals and medical practices	139 (156)	15% (16)
Financial sector, including banking, insurance, credit agencies and debt collectors	61 (80)	6% (8)
Other	331 (317)	34% (32)
TOTAL	968	100%

Age of complaints

Each year, we aim to complete 80 percent of our complaint investigations within nine months of receipt. Figure 2 shows we achieved our desired outcome by closing 91 percent within nine months. Of the remaining nine percent (85 files), five percent were closed before 12 months.

At year's end, work in progress totalled 247 files of which 92 percent were under nine months old.

Figure 2: Age of closed complaints 2010/11



Complaint outcomes

The focus of the complaints work is to provide a dispute resolution service as an alternative to court-based actions. Our investigators look for opportunities to motivate parties towards settlement of their issues to avoid the expense and stress of tribunal proceedings.

Table 5 shows the final outcomes on individual complaints closed during 2010/11. Some complaints have multiple outcomes. For example, a complaint may involve both collection and security issues. The collection issue might be resolved but the security issue may remain unresolved or not involve an interference with privacy.

TABLE 5: OUTCOMES ON CLOSED FILES 2010/11

Closed	No interference with privacy	Complaint has substance	Settled/mediated	Referred to Director of Human Rights Proceedings
999	686	313	281	19

We continue to measure our outcomes against the total number of complaints closed. We recognise, though, that even those complaints where there is no “interference with privacy” can involve a breach of a privacy principle. Those complaints can often provide opportunities for discussion and resolution between the parties, and can result in useful changes of practice. Initiating dialogue and achieving a mutual understanding can also enable the parties to deal with wider issues.

The majority of our complaints arise out of circumstances where privacy is not the only issue involved. For instance, many complaints involve the breakdown of workplace relationships, debt issues, criminal or enforcement investigations, or confusion with a health provider. Often we find that a complainant uses the privacy angle of a dispute as a last effort to achieve a desired outcome. While we are generally not able to resolve the wider issues in these cases, we often encourage understanding to allow the parties to move on from or to resolve the privacy aspect.

Top respondent agencies

Seven agencies generated more than 300 complaints to the Privacy Commissioner this year. Non-government agencies have not made the top respondent list for past three years.

Table 6 sets out the complaints received and the number closed throughout the year for top respondent agencies. In total, these agencies constitute nearly a third of the Privacy Commissioner’s complaints work.

TABLE 6: COMPLAINTS RECEIVED AND CLOSED FOR TOP RESPONDENT AGENCIES 2010/11

Agency	No of complaints received	No of complaints closed
New Zealand Police	69	82
Ministry of Social Development	64	72
Department of Corrections	63	63
Accident Compensation Corporation	60	61
Department of Labour (Immigration New Zealand)	45	54
Inland Revenue Department	12	9
NZ Security Intelligence Service	10	13
TOTAL	323	354

Table 7 shows the various outcomes on the complaints closed for each respondent.

Most of the agencies in this list carry very significant and often sensitive holdings of personal information. There is a notable increase in settlement outcomes for all of these agencies.

TABLE 7: OUTCOMES FOR TOP RESPONDENT AGENCIES 2010/11

Agency	Closed	No interference with privacy	Complaint has substance	Settled/mediated	Referred to Director of Human Rights Proceedings
New Zealand Police	82	57	25	19	6
Ministry of Social Development	72	48	24	20	2
Department of Corrections	63	41	22	19	1
Accident Compensation Corporation	61	45	16	15	1
Department of Labour (Immigration New Zealand)	54	23	31	31	0
Inland Revenue Department	9	3	6	6	0
NZ Security Intelligence Service	13	13	0	0	0

The Privacy Commissioner has oversight of the New Zealand Security Intelligence Service for access and correction issues only. The Service is not subject to our scrutiny under the collection, use or retention principles of the Act.

Satisfaction survey

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

We received 141 (last year, 256) surveys in response, made up of 84 (161) replies from complainants and 57 (95) from respondents.

The survey questions were the same as last year. Participants were asked to rate the various factors on a scale of 1 to 5, with the lower numbers representing negative comment and the higher numbers positive comment. We calculate a score of three or better as a party being satisfied, through to a score of five being very satisfied. The survey results were (last year's survey results in brackets):

- 77.5 percent (80) said they were satisfied or very satisfied with the service
- 91.5 percent (88.5) had expectations of a good to very good service
- 75 percent (78.5) felt their expectations were met or bettered
- 83 percent (83) agreed or strongly agreed that staff were competent
- 83.5 percent (88) agreed or strongly agreed that staff kept their promises
- 76.5 percent (78.5) agreed or strongly agreed that they were treated fairly
- 63.5 percent (68) agreed or strongly agreed that individual circumstances were considered
- 72 percent (75) agreed or strongly agreed that the service was good value for tax payer money.

The survey results are similar to last year's. We aim to provide a service where 80 percent or more of our parties rate our service as satisfactory or better.

External audit

We contracted a barrister, experienced in privacy issues, to audit a random selection of 20 complaint files to determine the quality of the investigations process. The features assessed were analysis of legal issues, clarity and sensitivity of communications and correspondence, and fairness and timeliness of the process.

Each file was awarded points between one and five with five being an excellent overall performance in managing the complaint. The total perfect score for all files would be 100.

The audited files scored a total of 91.5, compared to last year's total of 91. The average file score was 4.6. Twelve files scored a maximum of five points.

Litigation

Human Rights Review Tribunal

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

The 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 chance to resolve the dispute before engaging in litigation.

TABLE 8: REFERRALS, TRIBUNAL CASES AND OUTCOMES 2005-2011

	05/06	06/07	07/08	08/09	09/10	10/11
Referrals to Director of Human Rights Proceedings	12	15	20	12	18	17
New proceedings	17	22	19	29	13	25
Settled/withdrawn (in HRRT)	6	4	6	3	12	4
Costs awarded	–	5	5	4	2	6
Struck out	16	2	19	3	2	4*
No interference	5	4	4	6	5	5
Interference	5	3	0	1	2	3

*Three of the proceedings that were struck out involved the same plaintiff. He had been warned by the Tribunal that if he continued to send obscene and offensive correspondence, his claims would be deemed to be abandoned. He continued the behaviour, so his claims were dismissed.

We referred 17 complaints to the Director during the year. At the year's end, he was considering whether to take proceedings in 24 cases. He declined to take proceedings in three cases, and filed proceedings in five cases.

We decided not to refer 13 cases because we believed that either nothing would be gained by further scrutiny or that the formal evidence available was insufficient to support a successful case.

The Tribunal awarded compensation in all three cases in which it found that an interference with privacy had occurred. The cases were as follows:

- *Shahroodi v Civil Aviation Authority*. The Tribunal found that the CAA had not complied with Mr Shahroodi's rights to access information about himself, and made an award of \$10,000. The case is under appeal to the High Court.
- *AB v Ministry of Social Development*. The Tribunal found that the Ministry had failed to correct its file that contained an incorrect allegation that the plaintiff had a conviction for domestic violence. It made a compensation award of \$3,500.
- *Z v Commissioner of Police*. The plaintiff was involved in Family Court proceedings, during which the other party asked the Police for information about his history of domestic violence. The Police disclosed not only that information but also much wider information about his criminal history (most of which was irrelevant and related to events long before). The Tribunal found that the disclosure was excessive and, by a majority, awarded the plaintiff \$6,000.

In addition, the Tribunal issued an indicative decision in *SC v Auckland District Health Board*. The Tribunal said that, pending further evidence, it looked as if the Auckland District Health Board had taken insufficient steps to check the accuracy of allegations about the plaintiff's mental health before disclosing those allegations to Child Youth and Family. It indicated that an award of \$6,000 would be appropriate. No further evidence was received and no final decision was issued, because the parties settled the matter out of court.

Judicial review

The lengthy case of *Jeffries v Privacy Commissioner* concluded in August 2010, with the Supreme Court's decision that Mr Jeffries was required to provide the Privacy Commissioner with the information she had demanded under the Privacy Act. The Court said that it was for the Commissioner to make a decision about whether the information was legally privileged and, if so, to protect the privilege. However, Mr Jeffries had no basis to withhold the information from her.

The result means that, throughout the judicial review proceedings, all courts have upheld the actions of the Privacy Commissioner.

Employment Court

We were asked by the Employment Court to assist the Court in the case of *Massey University v Wrigley and Kelly*. The case involved internal restructuring at the University. Existing staff in a department had to reapply for fewer positions. The unsuccessful candidates asked to see information not only about the decision process and about the reasons why they were not reappointed, but also information about the successful candidates (interview notes made by the panel etc).

Requests for the information under either the Privacy Act or the Official Information Act would have allowed the University to withhold the information about the successful candidates. However, the Court decided that, although some of the information was confidential in nature, the University had to give it to the unsuccessful candidates as part of its obligations of good faith. The Court disagreed with our view that the ability to withhold confidential information to protect privacy under the Employment Relations Act should be aligned with the provisions of the Privacy Act.

Commissioner initiated inquiries

The Privacy Commissioner does not need to receive a complaint before she can investigate a matter that she believes may infringe privacy. She can open her own inquiries.

Many of these inquiries are simple exchanges of correspondence. For example, the Commissioner may ask an agency to explain how an incident occurred. She will receive the agency's response and if no further action appears necessary, that will be an end of the matter.

Occasionally, inquiries are more in-depth. Some result in a public statement or even a formal report on the outcome of the inquiry.

There were three Commissioner-initiated inquiries of note during this reporting year.

Google WiFi

In December 2010, we concluded our inquiry into Google's collection of WiFi information during its Street View filming in New Zealand. The report is available at <http://privacy.org.nz/google-s-collection-of-wifi-information-during-street-view-filming/>

The inquiry concluded that Google breached the Privacy Act when it failed to inform people of the collection of WiFi information. It also breached the Act by collecting payload information from unprotected WiFi networks.

Google significantly changed its privacy policies as a result of this and other similar inquiries overseas. It also made various other undertakings, listed in the report. One of the most important was that it undertook to securely delete the payload data that it collected in New Zealand. Google confirmed in early March 2011 that it had deleted that data; the deletion was independently verified.

Access to Telecom customer information by competitor

In January 2011, media reports alleged that a marketing company working for Slingshot had inappropriately accessed Telecom customer information through Telecom's "Wireline" portal. The allegation was that the company had used a Telecom dealer's login details and password. The security of the Wireline system was also called into question.

At time of writing this report, the inquiry was near to completion.

Audio-recording in taxis

In June 2011, there were media reports that some taxi companies intended to use audio recording facilities in cabs. Many taxi companies are required under new rules to install and operate video recording in taxis, for safety purposes. In some cases, the equipment is also capable of recording sound. The issue of sound recording had not arisen when the video recording rules were being developed.

Both drivers and passengers raised concerns with us about sound recording. Our view was that the additional intrusion involved in recording sound was generally not going to be justifiable. As a result, we advised taxi companies not to record sound without exceptionally good reasons. Within two weeks, we had also developed a guidance sheet for taxi companies about how to manage the privacy issues with sound recording (available at <http://privacy.org.nz/information-sheet-for-taxi-organisations/>). The guidance was distributed to taxi companies through NZTA as well as being available on our own website.

Section 54 authorisations

Section 54 of the Privacy Act allows the Commissioner to authorise actions that would otherwise be a breach of principles 2, 10 or 11, as long as the public interest or the benefit to the individual substantially outweigh the impact on privacy. The power to grant specific exemptions gives the Act extra flexibility.

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

This year, we received one application for a section 54 exemption, from the Earthquake Commission (EQC). EQC urgently wished to disclose information to

Housing New Zealand (HNZ) about the properties that had been worst affected by the Darfield earthquake on 4 September 2010.

HNZ had asked EQC to give it:

- the addresses of the worst affected properties (around 1300 addresses)
- information gathered by estimators, insurers and contractors doing repair work.

HNZ wanted to get the information so it could assess risks to its own properties and tenants, to assess welfare and recovery needs for its tenants, to talk to private owners next to endangered houses it owns, and so that it could assess the validity of any claims for emergency accommodation. EQC was uncertain whether it could supply the information without breaching the Privacy Act.

We responded to EQC the day after receiving the application. We pointed out that it was allowed to supply HNZ with information about its own properties, since supplying information to property owners was one of the purposes that EQC had the information. We also noted that if a person made an application for emergency housing to HNZ, HNZ at that time could get the person's authorisation to get any information it needed from EQC. There was therefore no need for us to grant a section 54 authorisation, since EQC could comply with the Privacy Act.

EQC and HNZ agreed that our approach was practicable, and withdrew the application.

In November, EQC made a further enquiry about whether it needed our authorisation to be able to publish maps of affected land. We advised them that, given the circumstances, public notification was one of the purposes that it had the information and that therefore a section 54 application was unnecessary.

Policy

We routinely provide advice on how to manage personal information in a variety of policy initiatives. Most of our advice is to government, but we also advise businesses on how to establish or improve their privacy practices.

Our advice to government includes:

- independent advice to Cabinet on decisions involving personal information
- advice to Cabinet and Parliamentary Select Committees on legislative changes involving personal information
- advice to departments on undertaking privacy analyses as part of wider policy initiatives.

Increasingly, Parliament is giving us statutory roles to supervise the implementation of legislation governing the use of personal information by government departments. A recent example is our consultative role on the use of biometric information under various sections of the Immigration Act 2009. While these roles can be resource-intensive, they can provide important assurance to the public that sensitive personal information is being responsibly managed by public sector organisations.

We were asked to advise on 79 new policy issues during the 2010/11 financial year (compared to 126 new policy issues in 2009/10). These figures appear to be closely aligned to the electoral cycle, and predictable peaks and troughs in government policy-making.

Many policy projects are not concluded by the agency within the financial year in which they come to us. The number of active issues – our work in progress – has remained relatively constant (192 in 2010/11 compared with 208 in 2009/10).

The overwhelming majority of requests (65 of the 79) for advice come from central government agencies. The nature of many requests suggests to us that public sector knowledge of the Privacy Act is uneven. Yet responsible stewardship of New Zealanders' personal information should be a key management responsibility within government. It is therefore concerning to see that many government agencies are still relying on us to advise them how to comply with the Privacy Act, and how to manage personal information in a way the public will trust. It is surprising that knowledge of the Privacy Act is not more commonly embedded in the agencies themselves.

We have started to produce some tools to help address this problem. During the 2010/11 financial year, we produced "Getting Started" - a guide to the principal questions that advisers need to answer to get privacy right. This user-friendly guide supplements the more comprehensive 2007 Privacy Impact Assessment Handbook and helps to introduce privacy impact analysis to a wider audience. Further work is needed, though, on understanding the causes of the uneven privacy capability in the public sector, and designing initiatives to improve it. The guide is available from our website, or, for public sector agencies, from the PSI site.

During 2010/11, we put in place new systems to try to assess the effectiveness of our advice to government departments, Cabinet, and Parliamentary Select Committees. We based this around an assessment of whether our advice was taken up. The take-up of the Office's advice shows that our role has produced specific improvements in processes for personal information handling in the public sector.

Across the 69 activities during the year where effectiveness could be assessed¹, our views resulted in some improvement or substantive improvement in 40 cases. We considered that no changes were required in a further 13 cases.

Legislation

Many of the policy projects we are involved in result in draft legislation. We provide advice during the drafting phase, and may also make submissions to Select Committees if necessary. We are regularly consulted on bills, regulations, supplementary order papers, and rules at various stages of their development or review.

Major legislative projects where the Office played a role in 2010/11 include:

- the Search and Surveillance Bill
- the Customs and Excise (Joint Border Management and Information Sharing) Bill
- the Taxation (Tax Administration and Remedial Matters) Bill
- the Courts and Criminal Matters Bill.

Health advice

Health information privacy raises specific issues of its own, particularly with a national and international push towards the development of electronic health records, and the expansion of regional clinical data repositories and shared care initiatives (including Whanau Ora). In recognition of this, we have a memorandum of understanding with the Ministry of Health, which partially funds a specialist position to provide advice to the Ministry and the wider sector on health privacy issues.

Particular projects this year have involved providing advice to the National Health IT Board on electronic health records, keeping close to proposed changes to national collections and the NHI, and advising on the use of information derived from infant bloodspot or "Guthrie" cards.

We have also maintained an active programme of awareness raising through speaking engagements and articles on privacy issues targeted at the health sector. We also produced a health information toolkit, to advise the public about their rights, and to advise the sector about how to manage its privacy obligations.

Technology advice

Our efforts to improve privacy practice in the private sector have been focused this year on supporting New Zealand business to better understand privacy risks

¹ Not all policy enquiries result in action that can be readily assessed for effectiveness. Some files are assessed multiple times – at the planning and development phase, at Cabinet stage, during the preparation of draft legislation, on review by Select Committee, and in implementation and review.

and solutions in order to realise the benefits of new technology. We keep a close watch on new and developing technologies so that we are well placed to deliver comprehensive and timely advice.

In February and March 2011, we undertook a survey of international disclosures and use of overseas-based ICT infrastructure by government departments and major New Zealand corporations. The survey revealed that many organisations are using overseas ICT infrastructure in order to conduct their business, but that some do not have adequate controls over the information provided to third parties. Response to the survey reinforced our view that there is significant demand from organisations in New Zealand for guidance on how to manage privacy issues in making use of 'cloud computing' services, which often make use of overseas-based ICT infrastructure. We intend to produce guidance on cloud computing and privacy during 2011/12 for users, or potential users, of cloud computing services.

While we did not repeat our Portable Storage Device survey in 2010/11, we followed up on key low scoring agencies about how they have implemented our recommendations from the May 2010 survey. We were satisfied with the steps being taken to improve their practice in managing the risks to personal information from portable storage devices.

Law Commission's review of privacy

The Law Commission completed its four and a half year project on privacy near the end of the reporting year. The four-stage review looked at privacy values, changes in technology, international trends, and their implications for New Zealand civil, criminal and statute law. The final report (*Stage 4: Privacy Act*) was publicly released in early August 2011.

Key changes recommended in the report include:

- requiring that people be notified of serious security breaches, so that they can take steps to protect themselves
- enabling compliance notices to be issued to stop a business or government agency continuing to flout the law
- a national "Do-Not-Call" register to put a stop to unwanted telemarketing
- regulating surveillance, interception and electronic tracking
- streamlining privacy complaint processes to get faster resolution
- enabling the Privacy Commissioner to direct an agency to release information that it cannot legally withhold
- better processes to tackle systemic problems that affect many people, for instance by using representative or "class action" complaints

- narrowing the “domestic affairs” exemption in the Privacy Act to better protect people from publication of offensive or harmful material online
- making companies in New Zealand more clearly accountable if sending information offshore
- better regulating the way personal information is shared between government agencies through approved information sharing programmes.

The Stage 4: Privacy Act report, and the other reports making up the Law Commission’s review are available at: www.lawcom.govt.nz

The Minister of Justice has presented the report to Parliament (www.parliament.govt.nz) and the Government’s response is expected in early 2012.

Information matching

The Office has an important role in reviewing proposals by public sector agencies to match records from their databases, known as “information matching”. We provide assistance to agencies that are running, or planning to run, information matching programmes to help them understand the requirements of the Privacy Act. We monitor and report their compliance with those requirements.

Details of our information matching activities this year and reports on the 47 authorised programmes are in section 5.

Codes of practice

At the start of the year, there were five codes of practice in force. This included the Credit Reporting Privacy Code 2004, which was amended during the year. A new code, the Christchurch Earthquake (Information Sharing) Code 2011 (Temporary) was issued, amended and then expired.

Credit Reporting Privacy Code

The Office undertook a thorough review of the code after it had been in effect for two years. We examined complaints and enquiries to the Office, had discussions with the industry, reviewed international literature and developments and, most particularly, explored the issues with a specially convened external reference group.

The invited members of the reference group brought a diversity of backgrounds and viewpoints to the review. While several members were from the industry (both credit reporters and users of their services) there were also members from consumer groups, government and civil society. The reference group met a number of times as well as video conferencing between Auckland and

Wellington. We appointed an independent facilitator to help to assess and record the key issues.

As a result of the review, we made decisions to amend the code so New Zealand could move to more comprehensive credit reporting. By coincidence, reviews of privacy and credit law in Australia led the Australian Government to move in a similar direction. We studied Australian research findings and policy decisions and decided to remain broadly in line with Australia, given the closeness of the economies and the trans-Tasman connections in the credit reporting and banking industries.

We decided to amend the code in two stages due to delays in progress of the Australian reforms. The first stage included a public submission process during 2010 and Amendment No.4 was issued in December 2010.

After release of a draft Australian law, Amendment No.5 was publicly notified as a proposal in May 2011. At the end of the reporting year, we arranged public hearings with the intention that if the amendment were issued, it would come into force at the same time as Amendment No.4, in April 2012.

Together, the amendments will represent a fundamental shift in credit reporting in New Zealand. For the first time, the new system will let credit reporters collect information on the actual amounts of credit extended to individuals. Lenders will also be able to upload information to credit reporters, on a monthly basis, to show whether individuals have met their monthly credit repayments.

This new system will amass much larger collections of detailed and sensitive financial information on New Zealanders. There is therefore a strong need to make sure that individuals' interests are appropriately protected. We have introduced special provisions to try to ensure a high level of compliance, to make sure that individuals are fully informed about the process and that access to the information is strictly controlled. In addition, a new system of 'credit freezes' will be available for individuals who are at special risk of identity fraud.

The pay-off for New Zealand and individuals should be an enhanced ability to assess creditworthiness. International evidence suggests that this can bring economic benefits in terms of risk management for business and improved credit arrangements for individuals.

Christchurch Earthquake (Information Sharing) Code 2011 (Temporary)

On Tuesday 22 February 2011 a magnitude 6.3 earthquake struck the Canterbury region causing substantial damage to Christchurch and killing 181 people. The Government declared a state of national emergency the next day and the Privacy Commissioner issued the temporary Christchurch Earthquake (Information Sharing) Code within 48 hours of the earthquake, under special urgency powers.

The code was a precaution to ensure that agencies involved in responding to the emergency, and other agencies interacting with them and with victims' families, knew they had the authority to share personal information as needed. It was not a reaction to specific problems. Instead, it was a pre-emptive action to lessen the chances that unnecessary barriers to disclosure could arise. It was based on overseas experience, studies and legislative provisions.

In particular, the code provided that in addition to any existing lawful reason for disclosing personal information, information could be disclosed for a 'permitted purpose' that directly related to the government and local government response to the Christchurch earthquake emergency. In particular, a permitted purpose included:

- identifying individuals who are or may be injured, missing or dead as a result of the emergency
- assisting individuals involved in the emergency to obtain services such as repatriation, medical treatment, financial or other humanitarian assistance
- assisting with law enforcement in relation to the emergency
- coordinating and managing the emergency
- ensuring that responsible people (such as parents, spouses, partners and nominated contact points) are appropriately informed of matters related to individuals affected by the emergency.

Code expiry date

Initially the code was issued to expire with the state of national emergency. However, we realised that the state of emergency was renewed each week. This did not provide sufficient certainty for some agencies to be able to share information under the code, and therefore reduced the benefits that the code was intended to provide. Accordingly, we amended the code early in March to provide for a fixed expiry date of 24 May 2011, three months after commencement. This was extended to 30 June 2011. At that date, the code was allowed to lapse.

Dealing with matters of urgency under the Privacy Act

It was possible for the code to be issued and amended so quickly because of the special powers in the Privacy Act for dealing with matters of urgency. In such cases, public consultation can be dispensed with, although safeguards exist to ensure that the power is not open to abuse. Accordingly, codes issued in reliance upon such powers are temporary and not permanent. As is usual, the code and the amendments had to be tabled in Parliament. The Regulations Review Committee of Parliament provides oversight and can act if it has any concerns with the code. The Committee had no concerns.

Views on the Code

Although a public consultation process was not possible, the Commissioner sought others' views to ensure that the code was necessary, appropriate and useful. This included engaging a Christchurch lawyer to interview Christchurch government and local government employees and civil society organisations involved in the emergency response to ask about knowledge and use of, and attitudes to the code. We also undertook a survey of government departments known to be involved in the emergency response.

We published on our website letters to the Regulations Review Committee, the report of the interviews, and the results of our survey of government departments to help promote the transparency of the process of issuing the code. The published information showed a high level of support for the code as an appropriate and proportionate response to the emergency. We were told that there was no need for any long term exemption from the privacy law but the additional flexibility provided in the short term by the code was greatly valued by staff of the agencies responding to the emergency.

The ongoing need for information collection, use and disclosure, in responding to the welfare needs of victims of the emergency was seen as being well able to be accomplished within the normal constraints of the Privacy Act.

Consultations with the Ombudsmen

The Ombudsmen routinely consults 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.

This year we received 52 consultations from the Ombudsman and completed and closed 55. These figures represent a similar workload to that of the previous year, and a 100 percent increase on volumes before 2010. Most consultations (82 percent) were completed within 2 months of receipt.

The most topical consultation was about expenditure by public sector chief executives. We have worked closely with the Ombudsmen to provide some overall guidance about the scope of expenses information that ought to be released to the public. The privacy interests that gave rise to the most consultations were those dealing with employment issues within the government.

4: OFFICE OF THE PRIVACY COMMISSIONER

4: OFFICE 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.

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.

Staff

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

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

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

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

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

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

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

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. The Office has an EEO policy that is integrated with the human resource programmes outlined in the Statement of Intent 2010 and encourages active staff participation in all EEO matters. These are reviewed annually.

During the 2010/11 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).

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

TABLE 9: OFFICE OF THE PRIVACY COMMISSIONER
WORKPLACE GENDER PROFILE 2010/11

	Women		Men		Total
	Full-time	Part-time	Full-time	Part-time	
Commissioner	1				1
Senior managers	1		3		4
Team leaders	2	1	1		4
Investigating officers	4	1	1		6
Administrative support	5	3			8
Advisers (technology and policy)	2		4		6
Enquiries officers	1		1		2
Total	16	5	10		31

TABLE 10: OFFICE OF THE PRIVACY COMMISSIONER
WORKPLACE ETHNIC PROFILE 2010/11

	Māori		Pacific Peoples		Asian (including South Asian)		Other ethnic groups		Pakeha/ European	
	Full-time	Part-time	Full-time	Part-time	Full-time	Part-time	Full-time	Part-time	Full-time	Part-time
Commissioner									1	
Senior managers									4	
Team leaders									4	
Investigating officers					1				4	1
Administrative support									5	3
Advisers (technology and policy)									6	
Enquiries officers									2	

5: INFORMATION MATCHING

5: INFORMATION MATCHING

Information matching and privacy – an introduction

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

Information matching can be problematic from a privacy perspective because:

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

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

These controls include:

- ensuring that individuals are aware of the programme and that their information may be included in it (rule 1)
- limiting the disclosure and use of information (rule 4 and the purpose given in the specific statutory provision allowing the programme);
- limiting the retention of information (section 101 and rule 6)
- notifying individuals and allowing them time to challenge a decision before any action is taken against them (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 <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)	NZ Citizenship Office (part of DIA)
Corrections	Department of Corrections
CSC	Community Services Card
Customs	NZ 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)	NZ Passports Office (part of DIA)
RMVT	Registrar of Motor Vehicle Traders
SVB	Sociale Verzekeringsbank (Netherlands)
WfFTC	Working for Families Tax Credits (formerly Family Support Tax Credits)

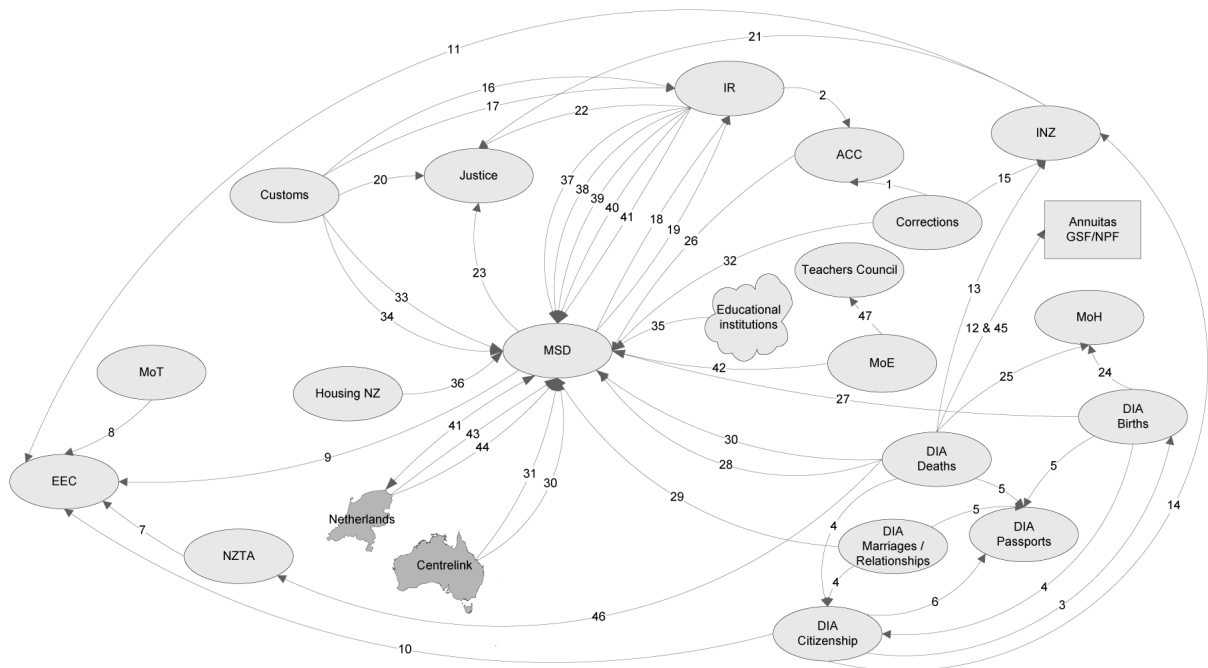
The year in information matching

Our oversight of information matching during the year included:

- monitoring 47 active programmes
- reporting to the Minister of Justice on a periodic review (s.106) of four information matching programmes
- reporting to the Minister of Justice on a proposed information exchange between Croatia and the Ministry of Social Development
- publishing new guidance about online transfers for information matching.

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

Figure 3: Active authorised information matching programmes 2010/11



Highlighted errors

MSD reporting

Between November 2008 and May 2009, MSD ran a one-off data match against historical death records provided by DIA. MSD matched the death records against their own records to identify cases of significant fraud where

superannuation payments were continuing to be paid to relatives of the deceased.

Although the matching of historic death records was authorised under an information matching agreement, details about the match run should have been provided to us under s.105(3) as part of reporting on matching activities in the 2008/09 year. We requested details from MSD in December 2010 following media coverage about convictions resulting from the match. Details of the results are included in the BDM/MSD Identity Verification Programme report on page 76.

Outreach

In May, the Office hosted an Information Matching Interest Group meeting. The National Programmes Centre of MSD presented an item about their work to enhance matching with Inland Revenue. An update on the Law Commission information sharing proposals was provided by this Office.

Also in May we published new guidance about how to set up online transfers for information matching. The guidance is available at <http://privacy.org.nz/how-to-set-up-online-transfers-for-information-matching/>.

We published two Information Matching Bulletins. Back copies are available at www.privacy.org.nz/information-matching-bulletins/.

The Office ran one information matching workshop in August 2010 for 13 people.

Changes in authorised and operating programmes

Parliament passed two new information matching authorisations during the year. An Order in Council was passed on 29 November 2010 to bring into force two provisions in the Immigration Act 2009. The two programmes are not yet active. They are:

- MSD/INZ Sponsorship Obligations Programme
- INZ/MoH Publicly Funded Health Eligibility Programme.

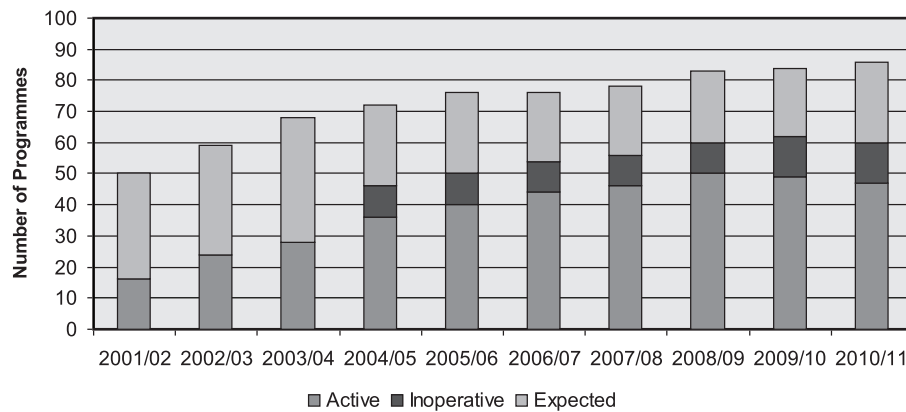
Five programmes are not reported on as they have not been active this year. They are:

- Netherlands/MSD Debt Recovery Programme
- Employers/MSD section 11A Social Security Act Programme
- BDM(Births)/MoE Student Birth Confirmation Programme
- Customs/MED Motor Vehicle Traders Importers Programme
- MoT/MED Motor Vehicle Traders Sellers Programme.

The BDM(Deaths)/Justice(MLC) Maori Land Title Succession Programme has been on hold since 2008. Justice has no plans to resume matching at present.

The IR/MSD Debtor Tracing Programme ceased operation in June 2011.

Figure 4: Authorised, operating and inoperative information matching programmes 2002-2011



The strong growth in new operating programmes between 2001 and 2008 has stalled with some existing programmes permanently ceasing operation, or being on hold temporarily because of human resource constraints. But some programmes have grown in scope. For example, MSD now uses information from the Corrections, Customs, and ACC programmes for the additional purpose of debt recovery.

Periodic review (s.106) of information matching programmes

In April we reported to the Minister of Justice on a periodic review (s.106) of four information matching programmes (IR/MSD Debtors Tracing; MSD/IR Working for Families Tax Credits; INZ/EEC Unqualified Voters; MSD/Justice Fines Defaulters). We recommended that three programmes should continue, and the IR/MSD Debtors Tracing Programme should be further reviewed because of poor performance. The programme has since been discontinued. Our report is available at <http://privacy.org.nz/information-matching-reports-and-reviews/>.

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 2011, 31 of the 47 active programmes used online transfers. As Tables 11 and 12 show, we issued two new authorisations this year, and 16 renewals.

TABLE 11 FIRST TIME APPROVALS 2010/11

User agency Programme name (and number) Approval date	Reason for granting	Grounds in support
Ministry of Health		
NHI and Mortality Register (programme 25) 29 July 2010	efficiency and security	acceptable controls
Ministry of Social Development		
Netherlands General Adjustment (programme 44) 19 April 2011	efficiency and security	acceptable controls

TABLE 12 RENEWED APPROVALS 2010/11

User agency Programme name (and number) Approval date	Reason for granting	Grounds in support
Department of Internal Affairs		
Citizenship by birth processing (programme 3) 1 April 2011	continued efficiency	satisfactory audit result acceptable controls
Electoral Enrolment Centre		
Unqualified voters (programme 11) 26 October 2010	efficiency; data quality	acceptable controls
Inland Revenue		
Student loan interest (programme 17) 3 June 2011	continued efficiency	satisfactory audit result acceptable controls
Ministry of Justice		
Customs fines defaulters alerts (programme 20) 31 August 2010	efficiency and technology enabled	satisfactory audit result acceptable controls
INZ fines defaulters alerts (programme 21) 31 August 2010	efficiency and technology enabled	acceptable controls
Ministry of Economic Development		
Motor vehicle traders sellers 24 February 2011	continued efficiency	satisfactory audit result acceptable controls

Ministry of Social Development		
Results of study (programme 42) 1 July 2010	continued efficiency	satisfactory audit result acceptable controls
Verification of study (programme 35) 1 July 2010	continued efficiency	satisfactory audit result acceptable controls
HNZ benefit eligibility (programme 36) 30 September 2010	efficiency and security	acceptable controls
Arrivals and departures (programme 33) 30 September 2010	efficiency and security	acceptable controls
Customs periods of residence (programme 34) 14 December 2010	continued efficiency	satisfactory audit result acceptable controls
Centrelink periods of residence (programme 31) 14 December 2010	continued efficiency	satisfactory audit result acceptable controls
Change in circumstances (programme 30) 14 December 2010	continued efficiency	satisfactory audit result acceptable controls
Verification of study (programme 35) 28 June 2011	continued efficiency	satisfactory audit result acceptable controls
Results of study (programme 42) 28 June 2011	continued efficiency	satisfactory audit result acceptable controls
Teachers Council		
Unregistered teachers (programme 47) 30 June 2011	efficiency and security	acceptable controls

Programme reports

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

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

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

1 Corrections/ACC Prisoners Programme

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

Year commenced: 2000

Features: Data is transferred weekly by online transfer.

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

2010/11 activity:

Match runs	52
Records received for matching	109,734
Possible matches identified	4,572
Overpayments established (number)	29
Overpayments established	\$21,209
Average overpayment	\$731
Challenges	0
Challenges successful	0

Compliance: Compliant.

2 IR/ACC Levies and Compensation Programme

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

Year commenced: 2002

Features: Data is transferred weekly by encrypted USB stick.

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

2010/11 activity:

Self-employed people's records received for matching	545,695
Employers' records received for matching	532,286
Invoices issued to self-employed people	442,986
Invoices (individual employee) issued to employers	583,489

Challenges by individuals	30
Challenges by corporations	65
Total challenges	95
Successful challenges	8

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.

2010/11 activity:

Births registered	64,871
Notices of adverse action	1,470
Challenges received	398
Successful challenges	292
Citizenship by birth declined	1,314

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

Commentary: Successful challenges to the accuracy of the matching process are significant at nearly 20 percent. Except for 2008/09 which was almost as high at nearly 18 percent, the normal rate is less than 12 percent. DIA is investigating the reasons for this variation.

Compliance: Compliant.

4 BDM/DIA(C) Citizenship Application Processing Programme

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

Year commenced: 2005

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

BDM disclosure to Citizenship (DIA): Possible matches from the Births, Deaths and Marriages (relationships) databases are displayed to Citizenship staff as they process each application. These details include full name, gender, birth date, birthplace and parents' full names.

2010/11 activity:

Applications for citizenship by descent (may include more than one person)	64,871
Notice of adverse action (arising from failure to match)	9
Successful challenges	9
Citizenship by descent registered	8,814

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

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

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

Compliance: Compliant.

5 BDM/DIA(P) Passport Eligibility Programme

Purpose: To verify, by comparing details with the Births, Deaths and Marriages registers, whether a person is eligible for a passport, and to detect fraudulent applications.

Year commenced: 2003

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

BDM disclosure to Passports (DIA): Possible matches from the Births, Deaths and Marriages (relationships) databases are displayed to Passports staff as they process each application. The details displayed include full name, gender and date of birth.

2010/11 activity:

Passport applications	596,672
Possible matches: Births	1,239,834
Possible matches: Marriage/Relationships	211,773
Possible matches: Deaths	2,337,341
Notice of adverse action	6,287
Successful challenges	6,141
Passports issued (diplomatic, official and standard)	603,669

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

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

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

Compliance: Compliant.

6 Citizenship/DIA(P) Passport Eligibility Programme

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

Year commenced: 2003

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

Citizenship (DIA) disclosure to Passports (DIA): Possible matches from the Citizenship database are displayed to Passports staff as they process each application. The possible matches may involve one or more records. The details displayed include full name, date of birth, country of birth and the date that citizenship was granted.

2010/11 activity:

Passport applications	596,672
Possible matches to Citizenship records	522,672
Notice of adverse action	778
Successful challenges	746
Passports issued (diplomatic, official and standard)	603,669

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

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

Compliance: Compliant.

7 NZTA/EEC Unenrolled Voters Programme

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

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

Year commenced: 2002

Features: Data transferred on request by CD.

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

2010/11 activity:

Match runs	2
Records received for matching	1,228,389
Invitations to enrol sent out	189,132
Invitations presumed delivered	169,973
New and updated enrolments	23,991
Percentage of letters delivered resulting in changes	14%
No response	145,982
Cost	\$104,387.61
Average cost per enrolment	\$4.35

Compliance: Compliant.

8 MoT/EEC Unenrolled Voters Programme

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

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

Year commenced: 2002

Features: Data transferred on request by CD.

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

2010/11 activity:

Match runs	2
Records received for matching	969,696
Invitations to enrol sent out	83,180
Presumed delivered	78,940
New and updated enrolments	14,990
Percentage of letters delivered resulting in changes	19%
No response	63,950
Cost	\$49,551.74
Average cost per enrolment	\$3.31

Compliance: Compliant.

9 MSD/EEC Unenrolled Voters Programme

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

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

Year commenced: 2002

Features: Data is 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.

2010/11 activity:

Match runs	2
Records received for matching	448,305
Invitations to enrol sent out	83,682

Presumed delivered	81,269
New and updated enrolments	14,729
Percentage of letters delivered resulting in changes	18%
No response	66,540
Cost	\$49,786.09
Average cost per enrolment	\$3.38

Compliance: Compliant.

10 Citizenship/EEC Unenrolled Voters Programme

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

Year commenced: 2002

Features: Data transferred on request by CD.

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

2010/11 activity:

Match runs	2
Records received for matching	10,600
Invitations to enrol sent out	437
Presumed delivered	427
New enrolments	64
Percentage of letters delivered resulting in changes	15%
No response	363
Cost	\$587.02
Average cost per enrolment	\$9.17

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, so their names may be removed from the roll.

Year commenced: 1996

Features: Data transferred online daily.

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

2010/11 activity:

Records received for matching (as at 30 June 2011)	211,672
Possible matches identified	1,618
Notice of adverse action sent	1,618
Challenge received	64
Successful challenges	56
Removals from roll	1,562
Cost	\$47,242.66
Average cost per removal	\$30.25

Commentary: In August the legislation was amended to allow the match to take place before people are added to the roll (previously the check could only occur after the person had been added to the roll).

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 every four weeks by CD.

BDM disclosure to GSF: BDM provides information from the Deaths Register covering the 12 weeks prior to the extraction date. The information 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).

2010/11 activity:

Records received for matching	30,650
Possible matches identified	9,009
Notices of adverse action sent	591
Challenges	2
Successful challenges	2

Commentary: Both challenges were verified as arising from mis-matches. In addition a mailing error occurred resulting in one notice being sent to the wrong address.

Compliance: Compliant.

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

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

Year commenced: 2007

Features: Data transferred every six months by CD.

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

2010/11 activity:

Records received for matching	28772
Possible matches identified	925
Records marked as deceased - overstayer list	117
Records marked as deceased - temporary visa holders' list	79
Total number of records updated as deceased	196

Compliance: Compliant.

14 Citizenship/INZ Entitlement to Reside Programme

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

Year commenced: 2004

Features: Data transferred every six months by CD.

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.

2010/11 activity:

Match runs	3
Records received for matching	1,135,611

Possible matches identified	2,848
Number of NZ citizens removed from the overstayer list	373

Commentary: In each of the last four years INZ has performed two match runs to cover grants of citizenship in the current period, and one match run to cover historical records previously received in earlier matches. The purpose of processing citizenship records previously received is to identify individuals who continue to travel using their non-New Zealand passport.

When returning to New Zealand using their non-New Zealand passport, Immigration officials do not know that these individuals have been granted citizenship, and have to grant a temporary visa based on the passport presented. The historical match allows Immigration to re-identify these individuals, and remove them as temporary visa holders in INZ's records.

Compliance: Compliant.

15 Corrections/INZ Prisoners Programme

Purpose: To identify prisoners who fall within the deportation provisions of the Immigration Act 2009 as a result of their criminal convictions, or are subject to deportation from the country because their visa to be in New Zealand has expired.

Year commenced: 2005

Features: Data transferred weekly by online transfer.

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

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

2010/11 activity:

Match runs	51
Possible matches identified	354
Cases excluded as not being eligible for removal or deportation	298
Notices of adverse action	56

Successful challenges	1
Cases considered for removal and deportation	51
Removals and deportations from NZ at year's end	29

Commentary: The Immigration Act 2009 was implemented on 29 November 2010. This year's figures include both removals and deportations commenced under the 1987 Act and progressed under the 2009 Act, and deportations commenced and progressed under the 2009 Act.

Last year we reported on an anomaly between Police and Corrections sentencing records. The Department for Courts (Courts) investigation to see if data transferred from their records to Corrections was involved could not be completed because Corrections was unable to provide the requested data. INZ advises that, along with Corrections, they will investigate any further issues on a case by case basis.

In March, we met with INZ and Corrections officials to be briefed on the steps taken to resolve data matching anomalies signalled in previous reporting. The anomalies relate to multiple aliases and old sentencing records appearing on data match reports.

The issue about multiple alias records was resolved by INZ modifying the data match report prior to it being provided to the compliance team. Corrections has identified a number of valid reasons why these old sentencing records can appear on match reports. INZ and Corrections advise they now have an arrangement in place for these anomalies to be dealt with as they are detected.

During the year we expressed concern to INZ about the routine retention of Corrections match information in an INZ operations report which appeared to breach the information matching rules. Following a review of the information contained in the report, INZ now removes the information we considered to be Corrections information once all immigration action is complete.

Compliance: Compliant but see comments.

16 Customs/IR Child Support Alerts Programme

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

Year commenced: 2008

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

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

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

2010/11 activity:

Possible matches identified	6264
Arrival cards received for liable parents	1080
Cards did not meet matching criteria	107
Cards illegible or incomplete	85
Remaining cards where contact attempted with liable parent	888
New contact details updated	300
Existing contact details confirmed	191
Contact details not useful	397

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

Compliance: Compliant.

17 Customs/IR Student Loan Interest Programme

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

Year commenced: 2007

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

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

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

2010/11 activity: An audit on the operation of this programme found that there are effective controls in place and no issues were identified.

There were 441,206 borrower records (384,434 last year) updated as a result of matching student borrower records with travel movement information held by Customs.

Commentary: Last year we raised concerns about the accuracy of reported figures. In November 2010 we met with IR officials to further discuss issues which occurred during the year. From those discussions we gained some reassurance that procedures have been improved and that information provided to us is accurate.

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 weekly by online transfer.

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

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

2010/11 activity: An audit on the operation of this programme found that there are effective controls in place and no issues were identified.

Because this programme operates as part of a complex business process aimed at ensuring WfFTC payments are made in a timely manner, it is difficult to quantify the scale of the match or identify trends in the number of matches made.

Compliance: Compliant.

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

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

Year commenced: 1995

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

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

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

2010/11 activity: An audit on the operation of this programme found that there are effective controls in place and no issues were identified.

IR does not routinely calculate savings for this programme. But data provided by IR as part of the formal review suggests that annual estimated savings from this programme are in the \$4m to \$5m range.

Commentary: This year we completed a formal review of this programme under s.106 of the Privacy Act. While we had reservations about the way IR calculates the estimated savings for this programme, we concluded that the authority to operate, conferred by section 84 of the Tax Administration Act 1994, should be continued.

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 daily by online transfer.

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

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 fines) has been issued.

Fines defaulters who have interception alerts recorded are those where:

- any amount of reparation is owing and a warrant to arrest (which covers part of the reparation outstanding) has been issued
- court-imposed fines of \$5,000 or more are outstanding and a warrant to arrest (which covers part of the court-imposed fines outstanding) has been issued.

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

2010/11 activity:

Silent alerts triggered	4,102
Individuals subject to silent alerts	1,808
Intercept alerts triggered	150
People intercepted	129
On departure	29
On arrival	113
Incorrect intercepts	18
Fines had already been paid	6
Wrong person identified by the match	12
Interception not completed	7
Fines received	\$88,154
Reparation received	\$101,367
Amount under a current time to pay arrangement	\$71,502
Remittals/ Alternative sentence imposed	\$140,458

Commentary: Justice suggest the 50% increase in interception alerts triggered this year resulted from a large number of new people becoming eligible for the Collection of Fines at Airports initiative following projects to review fines defaulter records.

While actual interceptions (129) doubled from last year (64), the value of outstanding fines and reparation received is about the same. Justice suggest this is because the average amount owed by those intercepted this year (\$4,839) was a lot less than the average amount owed by those intercepted last year (\$15,625). Amounts under a current time to pay arrangement dropped from \$397,249 (incorrectly reported as \$669,609 last year) to \$71,502.

As at 30 June, there were 2,888 fines defaulters who had interception alerts recorded against their names in Customs records, a slight increase over last year (2,800).

Compliance: Compliant.

21 INZ/Justice Fines Defaulters Tracing Programme

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

Year commenced: 2006

Features: Data transferred weekly by online transfer.

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

2010/11 activity:

Records sent to INZ	3922
Notices of adverse action	1276
Successful challenges	16
Payment received for fines	\$585,858
Amounts under a current time-to-pay arrangement	\$396,917
Remittals / alternative sentence imposed	\$613,183

Commentary: Justice suggests that the doubling of records sent to INZ this year resulted from a large number of new people becoming eligible for the CoFaA initiative following projects to review fines defaulter profiles.

Justice suggests projects to review fines defaulter profiles are likely to be behind the large increase (\$332,229) in remittals/alternative sentences imposed.

Fines payments received increased by about \$300,000 this year on a 60% increase in the number of notices of adverse action sent.

Conversely, amounts under a current time-to-pay arrangement have dropped by 35%. Justice advises that it is monitoring this downward trend.

Compliance: Compliant.

22 IR/Justice Fines Defaulters Tracing Programme

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

Year commenced: 2002

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

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

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

2010/11 activity:

Match runs	6
Records sent for matching	65,095
Possible matches identified	36,708
Notices of adverse action	29,113
Challenges	94
Successful challenges	40
Collection instituted	7,458
Amount paid or settled	\$3,744,129

Commentary: Last year we reported that a system fault and resource issues limited the amount of matching undertaken. The problems from last year have now been resolved and matching activity is increasing.

This programme is expected to go to a daily matching cycle in the next reporting period.

Compliance: Compliant.

23 MSD/Justice Fines Defaulters Tracing Programme

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

Year commenced: 1998

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

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

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

2010/11 activity:

Match runs	1
Records sent for matching	14,793
Possible matches identified	2,613

Notices of adverse action	2,479
Challenges	33
Successful challenges	5
Collection instituted	819
Amount paid or settled	\$121,884

Commentary: The sole match run was undertaken in February 2011. This is the first match run since June 2009 because of system issues at Justice, and system changes at MSD.

This year we completed a formal review of this programme under s.106. We concluded that the programme provides Justice with significant recoveries and the authority to operate conferred by section 126A of the Social Security Act 1964 should be continued.

Compliance: Compliant.

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

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

Year commenced: 2009

Features: Data transferred monthly 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 indicate whether the baby was stillborn.

2010/11 activity:

Records received for matching	69,067
Possible matches identified	69,047
Records not matched	20

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

Compliance: Compliant.

25 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.

2010/11 activity:

Records received for matching	29,501
Possible matches identified	26,005
Records manually matched	3,307
New NHIs allocated	189
Corrections to matches (including from previous years matches)	28

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

Compliance: Not compliant.

26 ACC/MSD Benefit Eligibility Programme

Purpose: To identify individuals whose MSD entitlement may have changed because they are receiving ACC payments, and to assist MSD in the recovery of outstanding debts.

Year commenced: 2005

Features: Data transferred weekly by online transfer.

ACC disclosure to MSD: ACC selects individuals who have:

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

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

2010/11 activity:

New match runs started in the reporting period	
Match runs	53
Records received for matching	1,952,282
Possible matches identified	5,836
Notifications received for debt recovery (from 30 May)	568
All match runs active in the reporting period	
Matches that required no further action	3,856
Notices of adverse action	1,914
Challenges	50
Successful challenges	33
Overpayments established	1,319
Value of overpayments established	\$1,658,024

Commentary: On 30 May 2011, MSD started using information received through this programme to assist it in the recovery of outstanding debts. Detailed reporting on this activity will commence in the next annual report.

Compliance: Compliant.

27 BDM/MSD Identity Verification Programme

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

Year commenced: 2007

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

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

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

2010/11 activity:

Benefit applications processed	404,153
Possible matches identified	10,524

Matches that required no further action	1,277
Letters advising update of information	497
Notices of possible adverse action	18
Challenges	0
Overpayments established	0
Value of overpayments established	0
Cases referred for further investigation	36

Commentary: MSD is unaware of the reason behind a sharp drop in the number of cases referred for further investigation (184 last year).

Historical data matching exercise completed

Between November 2008 and May 2009, MSD ran a one-off historical data match to identify cases of significant fraud where superannuation payments were continuing to be paid to relatives of the deceased.

Although the matching of historic death records was authorised under an information matching agreement, details about the match run should have been provided to OPC under s.105(3) as part of reporting on matching activities in the 2008/09 year. We requested details from MSD in December 2010 following media coverage about convictions resulting from the match.

The following is a summary of the historic match results.

Date range of death records	1 January 1984 – 12 December 2007
Records received for matching	654,906
Suspected fraud cases progressed	34
Challenges received	1
Successful challenges	1 (client still alive)
Overpayments established	33
Value of overpayments established	\$3,048,038

Of the 33 cases, 10 were found to be non-fraudulent and 95% of the money overpaid for those cases has been recovered from the bank account or the estate of the deceased. Criminal charges were laid against 16 of the 33, with the remaining seven cases not prosecuted because of insufficient evidence or because the individual responsible is now deceased.

Compliance: Compliant.

28 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 weekly by online transfer.

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

2010/11 activity:

New match runs started in the reporting period	
Match runs	52
Records received for matching	29,716
Possible matches identified	4,969
All match runs active in the reporting period	
Matches that required no further action	2,444
Notices of adverse action	2,401
Challenges	0
Overpayments established	270
Value of overpayments established	\$305,432

Compliance: Compliant.

29 BDM (Marriages)/MSD Married Persons Programme

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

Year commenced: 2005

Features: Data transferred weekly by online transfer.

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

2010/11 activity:

New match runs started in the reporting period	
Match runs	52
Records received for matching	22,695

Possible matches identified	3,018
All match runs active in the reporting period	
Matches that required no further action	1,799
Notices of adverse action	1,225
Challenges	1
Successful challenges	1
Overpayments established	482
Value of overpayments established	\$631,374

Compliance: Compliant.

30 Centrelink/MSD Change in Circumstances Programme

Purpose: To transfer applications for benefits and pensions and details of changes in circumstances between MSD and Centrelink (the Australian Government agency administering social welfare payments).

Year commenced: 2002

Features: Data is 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.

2010/11 activity:

Changes of information received by MSD from Centrelink	530,175
Notices of adverse action	6,967
Changes of information sent by MSD to Centrelink	218,534

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

Commentary: The audit on the operation of this programme noted that two online transfer systems are used. We were not aware of the second method when we issued the online transfer approval in December 2010. We are liaising with MSD to get updated documentation covering the second transfer method and to agree appropriate security conditions.

The second issue identified was that some records were not being destroyed within the appropriate timeframes. This has since been corrected. Otherwise the audit found there are effective controls in place.

Compliance: Not compliant.

31 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 is transferred monthly by online transfer.

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

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

2010/11 activity:

Records received back from Centrelink	8,094
Australian pensions granted	0

Notices of adverse action are recorded under the Centrelink/MSD Change in Circumstances Programme [see programme 30 on page 79].

Commentary: An audit on the operation of this programme found that some records were not being destroyed within the appropriate timeframes. This has since been corrected. Otherwise the audit found there are effective controls in place.

Compliance: Compliant.

32 Corrections/MSD Prisoners Programme

Purpose: To detect people who are receiving income support payments while imprisoned, and to assist MSD in the recovery of outstanding debts.

Year commenced: 1995

Features: Data transferred daily by online transfer.

Corrections disclosure to MSD: Each day, all prisoners who are received,

on muster or released from prison are included in the extraction file. Details disclosed include the full name (including aliases), date of birth, prisoner unique identifier and prison location, along with incarceration, parole eligibility date and statutory release date.

2010/11 activity:

New match runs started in the reporting period	
Match runs	358
Records received for matching	17,445,999
Possible matches identified	16,003
Notifications received for debt recovery (from 30 May)	1,437
All match runs active in the reporting period	
Matches that required no further action	6,566
Notices of adverse action	9,444
Challenges	8
Successful challenges	5
Overpayments established	3,151
Value of overpayments established	\$427,835

Commentary: On 30 May 2011, MSD started using information received through this programme to assist them in the recovery of outstanding debts. Detailed reporting on this activity will commence in the next annual report.

Compliance: Compliant.

33 Customs/MSD Arrivals and Departures Programme

Purpose: To identify current clients who leave for or return from overseas while receiving income support payments, and to assist MSD in the recovery of outstanding debts.

Year commenced: 1992

Features: Data transferred weekly by online transfer.

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

2010/11 activity

New match runs started in the reporting period	
Match runs	52

Records received for matching	9,632,937
Possible matches identified	54,032
Notifications received for debt recovery (from 30 May)	3,953
All match runs active in the reporting period	
Matches that required no further action	19,451
Notices of adverse action	30,674
Challenges	237
Successful challenges	207
Overpayments established	28,325
Value of overpayments established	\$18,915,102

Commentary: This year, MSD more than doubled the number and value of overpayments established by this programme. In September, MSD decided to cease matching work on some client cases (in advance of system changes) with Inland Revenue, and reallocate resources to this programme to clear a backlog of work.

On 30 May 2011, MSD started using information received through this programme to assist it in the recovery of outstanding debts. Detailed reporting on this activity will commence in the next annual report.

Compliance: Compliant.

34 Customs/MSD Periods of Residence Programme

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

Year commenced: 2002

Features: Data accessed online as required for individual enquiries.

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

2010/11 activity: MSD staff accessed 231 Customs records.

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

Compliance: Compliant.

35 Educational Institutions/MSD (StudyLink) Loans & Allowances Programme

Purpose: To verify student enrolment information to confirm entitlement to allowances and loans.

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

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

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

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

2010/11 activity:

Educational institutions involved in the matching programme	606
Records sent for matching	949,710
Individual applicants involved in matching	231,062
Notices of adverse action sent out (individuals may receive more than one)	47,136
Percentage of applicants issued a notice of adverse action	20%
Challenges	140
Successful challenges	62
Decisions to decline loan/allowance	26,316

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

Commentary: The decrease in educational institutions involved in this programme is primarily due to a decline in the number of secondary schools involved.

Compliance: Compliant.

36 HNZ/MSD Benefit Eligibility Programme

Purpose: To enable MSD to detect:

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

Year commenced: 2006

Features: Data transferred weekly 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 provided on termination of the tenancy.

2010/11 activity:

New match runs started in the reporting period	
Match runs	52
Records received for matching	88,471
Possible matches identified	6,492
All match runs active in the reporting period	
Matches that required no further action	6,381
Notices of adverse action	79
Challenges	0
Overpayments established	48
Value of overpayments established	\$76,355

Commentary: This programme continues to identify only a fraction of the 2005 forecast of \$1.4 million in annual overpayments. The on-going low return suggests double-dipping of housing assistance from Housing New Zealand and Accommodation Assistance from MSD is minimal. We suggest that MSD should consider the return on investment this programme provides.

Compliance: Compliant.

37 IR/MSD Commencement/Cessation Benefits Programme

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

Year commenced: 1993

Features: Data is transferred monthly by online transfer. A maximum of 100,000 records are allowed per supply.

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

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

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

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

2010/11 activity:

New match runs started in the reporting period	
Match runs	12
Records sent for matching	189,562
Possible matches identified	37,804
All match runs active in the reporting period	
Matches that required no further action	14,527
Notices of adverse action	11,194
Challenges	474
Successful challenges	64
Overpayments established	4,097
Value of overpayments established	\$13,421,905

Commentary: This year, MSD increased the frequency of matching from six times per year to monthly. But the overall numbers of records sent have been reduced. MSD has also introduced new business rules to help it select records using a risk based approach.

From November 2010, information received from IR was enhanced to include monthly gross income details and 'trading as' information. The enhanced information enables MSD to make more informed decisions about which records to investigate.

Under these new processes, MSD has reduced the number of successful challenges to notices of adverse action, and increased the value of overpayments established.

Just prior to the new matching processes in November, MSD decided to cease working on existing cases that did not have the enhanced information. This affected seven match runs which were at various stages of completion. MSD sent letters to those clients who had been in contact about their cases to inform them that no further action was to be taken.

Compliance: Compliant.

38 IRD/MSD Commencement/Cessation Students Programme

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

Year commenced: 2005

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

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

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

2010/11 activity:

New match runs started in the reporting period	
Match runs	11
Records sent for matching	57,075
Possible matches identified	25,570
All match runs active in the reporting period	
Matches that required no further action	7,725
Notices of adverse action	15,220
Challenges	423
Successful challenges	279
Overpayments established	5,510
Value of overpayments established	\$5,013,074

Commentary: The number of challenges has dropped by two thirds (1244 last year). MSD believes work done to improve the clarity of their client letters and better screening processes to identify potential overpayments may be behind

the drop in challenges.

Compliance: Compliant.

39 IR/MSD Community Services Card Programme

Purpose: To identify people who qualify for a Community Services Card (CSC) based on their level of income and number of children.

Year commenced: 1992

Features: Data is transferred fortnightly by USB stick.

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

2010/11 activity:

Match runs	50
Records received for matching	2,188,194
CSCs automatically renewed	298,672
'Invitation to Apply' forms sent out	88,743
Notices of adverse action	30,758
Challenges	67
Challenges successful	63

Commentary: Following the identification of errors in data extracted for this match in 2009/10, IR has continued to investigate the income information it reports to MSD. It has identified a further inconsistency in the definitions of income that may have understated income for an estimated 1,100 card holders. This means some cards may have been issued to people who are not entitled to them. IR is working with the Ministry of Health (as providing access to health subsidies is the primary function of Community Service Card) and MSD to clarify the appropriate definitions of income by 1 April 2012.

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

40 IR/MSD Debtors Tracing Programme

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

Year commenced: 1994

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

MSD disclosure to IR: MSD provides IR with the full name, date of birth, MSD client number and IRD number of 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.

2010/11 activity:

Match runs	6
Records sent for matching	196,362
Matches potentially useable	39,214
Notices of adverse action	1,689
Debt pursued	\$6,242,599
Repayments received by 30 June of reporting year	\$153,607
Total variable costs incurred	\$48,000

Commentary: MSD has decided to cease running this match. In response to an OPC assessment of the match in accordance with s106 of the Privacy Act, and an internal review by MSD, MSD recognised that this match was no longer effective and that it could obtain the information from other sources. The last match was run on 2 May 2011.

Compliance: Compliant.

41 IR/MSD (Netherlands) Tax Information Programme

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

Year commenced: 2003

Features: Data provided manually as required.

IR disclosure to Netherlands: For New Zealand-resident clients of the Netherlands government insurance agencies, IR provides the individual's contact details and income information to the Netherlands Sociale Verzekeringsbank (social insurance) or Uitvoeringsinstituut Werknemers Verzekeringen (employee insurance). MSD acts as liaison, forwarding requests to IR and forwarding the response to the Netherlands.

2010/11 activity: 55 requests for information were received and forwarded to IR, and the subsequent responses passed back to the Netherlands.

Commentary: MSD has previously reported only one request each year as the requests are all received in a single envelope. An audit on the operation of this

programme found that there are effective controls in place and no issues were identified.

Compliance: Compliant.

42 Ministry of Education/MSD (StudyLink) Results of Study Programme

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

Year commenced: 2006 (allowances) 2010 (loans)

Features: Data is transferred daily by online transfers.

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

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

2010/11 activity:

Allowance applications

Matching requests	82,222
Individual applications involved in matching	62,248
Notices of adverse action sent out	5,120
Successful challenges	1,892

Matching requests for allowance applications are repeated if necessary.

Loan applications

Records sent for matching	13,291
Applicants sent notices of adverse action	447
Successful challenges	137

Loan applications are matched only once.

Commentary: New eligibility criteria for student loans took effect during the year.

Almost all challenges are resolved by contacting the applicant for clarification.

Individuals may make more than one application for loans and/or allowances in a year. Notices of adverse action are sent when Studylink cannot satisfactorily match the information supplied or when the record indicated eligibility criteria

have not been met. More than one adverse action letter may be sent for an application (for example a notification letter and subsequently a letter declining their application). The application may be reinstated if the student provides additional information about their study history, or successfully applies for an exemption. This is recorded as a successful challenge.

Compliance: Compliant.

43 Netherlands/MSD Change in Circumstances Programme

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

Year commenced: 2003

Features: Manual transfer of completed application forms as required.

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

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

2010/11 activity: As an indicator of activity, MSD issued 344 notices of adverse action. This figure includes some corrections to SVB reference numbers. There were no challenges to these notices.

Commentary: An audit on the operation of this programme identified that the letter advising clients of changes did not include the statement informing clients of the adverse action that could be taken against them as a result of the information match. This statement was omitted during changes made during the year. MSD has committed to reinstating it by 21 November 2011. For this reason, the match was not compliant.

Compliance: Not compliant.

44 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 is transferred four times each year; from April 2011 online and previously by CD.

MSD disclosure to Netherlands: For MSD clients in receipt of both New

Zealand and Netherlands pensions, MSD provides the Netherlands Sociale Verzekeringsbank (SVB) with the changed superannuation payment information, the MSD client reference number and the Netherlands unique identifier.

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

2010/11 activity: MSD made deductions from pension payments to 3,622 people. There were 1,199 MSD clients resident in the Netherlands.

Commentary: An audit on the operation of this programme identified that the letter advising clients of changes did not include the statement informing clients of the adverse action that could be taken against them as a result of the information match. This statement was omitted during changes made during the year. MSD has committed to reinstating it by 21 November 2011. The potential adverse action is a reduction in New Zealand's contribution to the client's superannuation payments equal to the increase in the Netherlands contribution to the payments. An online transfer was granted in April 2011. Previously, data was sent by CD.

Compliance: Not compliant.

45 BDM(Deaths)/NPF Eligibility Programme

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

Year commenced: 2009

Features: Data transferred every four weeks by CD.

BDM disclosure to NPF: BDM provides information from the Deaths Register covering the 12 weeks prior to the extraction date. The information 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).

2010/11 activity:

Records received for matching	34,348
Possible matches identified - Pensioners	701
Possible matches identified - Contributors	393
Notices of adverse action sent	1,094
Challenges	0

Compliance: Compliant.

46 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 fortnightly by online transfer.

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

2010/11 activity:

Match runs	26
Records received for matching	29460
Possible matches identified	18588
Notices of adverse action	11614
Challenges	0
Successful challenges	0
Courtesy letters sent	5082
Driver licence records cancelled	17147

Commentary: The number of adverse action and courtesy letters sent is less than the number of driver licence records cancelled as some letters are withdrawn during the matching process following contact with the family through other channels.

Compliance: Compliant.

47 MoE/Teachers Council Registration Programme

Purpose: To ensure teachers are correctly registered and paid correctly.

Year commenced: 2010

Features: Data transferred up to fortnightly by online transfer.

MoE disclosure to Teachers Council: MoE provides full names, date of birth, gender, address, school(s) employed at, registration number (if known), and MoE employee number.

Teachers Council disclosure to MoE: The Teachers Council provides full names, date of birth, gender, address, registration number, registration expiry date, registration classification and MoE employee number (if confirmed).

2010/11 activity:

Match runs	6
Average number records received from MoE	51,768
Matched, letter sent to establish registration status	1,909
Match successfully challenged	60
Not matched, letter sent	570
Match resolved by teacher response	278
Remaining issues	261
Number of confirmed matches	986
Number of salaries adjusted	0

Commentary: This match commenced during the year and the processes are still being implemented and refined. Matching and consequent follow-up activities were undertaken as resources permitted and are expected to move to a fortnightly basis next year. MoE has not yet identified any errors in allowances based upon this match.

An audit on the operation of the online transfer system of this programme found that the conditions to provide security for the transfer were complied with.

Compliance: Compliant.

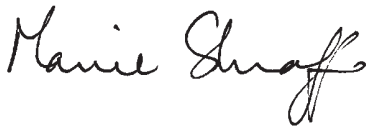
6: FINANCIAL & PERFORMANCE STATEMENTS

STATEMENT OF RESPONSIBILITY

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

The Privacy Commissioner has the responsibility for establishing, and has established, a system of internal control designed to provide reasonable assurance as to the integrity and reliability of financial and service performance 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 2011.



Privacy Commissioner

M Shroff

27 October 2011



General Manager

G F Bulog

27 October 2011

Independent Auditor's 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 2011

The Auditor-General is the auditor of the Office of the Privacy Commissioner (the Privacy Commissioner). The Auditor-General has appointed me, Leon Pieterse, using the staff and resources of Audit New Zealand, to carry out the audit of the financial statements and statement of service performance of the Privacy Commissioner on her behalf.

We have audited:

- the financial statements of the Privacy Commissioner on pages 105 to 131, that comprise the statement of financial position as at 30 June 2011, the statement of comprehensive income, statement of changes in equity and statement of cash flows for the year ended on that date and notes to the financial statements that include accounting policies and other explanatory information; and
- the statement of service performance of the Privacy Commissioner on pages 98 to 104.

Opinion

In our opinion:

the financial statements of the Privacy Commissioner on pages 105 to 131:

- comply with generally accepted accounting practice in New Zealand; and
 - fairly reflect the Privacy Commissioner's:
 - financial position as at 30 June 2011; and
 - financial performance and cash flows for the year ended on that date.
- the statement of service performance of the Privacy Commissioner on pages 98 to 104:
 - complies with generally accepted accounting practice in New Zealand; and
 - fairly reflects, for each class of outputs for the year ended 30 June 2011, the Privacy Commissioner's:
 - service performance compared with the forecasts in the statement of forecast service performance for the financial year; and
 - actual revenue and output expenses compared with the forecasts in the statement of forecast service performance at the start of the financial year.

Our audit was completed on 27 October 2011. This 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 our responsibilities, and we explain our independence.

Basis of opinion

We carried out our audit in accordance with the Auditor-General's Auditing Standards, which incorporate the International Standards on Auditing (New Zealand). Those standards require that we comply with ethical requirements and plan and carry out our audit to obtain reasonable assurance about whether the financial statements and statement of service performance are free from material misstatement.

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.

An audit involves carrying out procedures to obtain audit evidence about the amounts and disclosures

in the financial statements and statement of service performance. The procedures selected depend on our judgement, including our assessment of risks of material misstatement of the financial statements and statement of service performance, whether due to fraud or error. In making those risk assessments; we consider internal control relevant to the Privacy Commissioner's preparation of the financial statements and statement of service performance that fairly reflect the matters to which they relate. We consider internal control in order to design audit procedures that are appropriate in the circumstances but not for the purpose of expressing an opinion on the effectiveness of the Privacy Commissioner's internal control.

An audit also involves evaluating:

- the appropriateness of accounting policies used and whether they have been consistently applied;
- the reasonableness of the significant accounting estimates and judgements made by the Privacy Commissioner;
- the adequacy of all disclosures in the financial statements and statement of service performance; and
- the overall presentation of the financial statements and statement of service performance.

We did not examine every transaction, nor do we guarantee complete accuracy of the financial statements and statement of service performance. We have obtained all the information and explanations we have required and we believe we have obtained sufficient and appropriate audit evidence to provide a basis for our audit opinion.

Responsibilities of the Privacy Commissioner

The Privacy Commissioner is responsible for preparing financial statements and a statement of service performance that:

- comply with generally accepted accounting practice in New Zealand;
- fairly reflect the Privacy Commissioner's financial position, financial performance and cash flows; and
- fairly reflect its service performance.

The Privacy Commissioner is also responsible for such internal control as is determined necessary to enable the preparation of financial statements and a statement of service performance that are free from material misstatement, whether due to fraud or error.

The Privacy Commissioner's responsibilities arise from the Crown Entities Act 2004.


Responsibilities of the Auditor

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

Independence

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

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



Leon Pieterse
Audit New Zealand
On behalf of the Auditor-General
Auckland, New Zealand

Matters relating to the electronic presentation of the audited financial statements

This audit report relates to the financial statements of the Office of the Privacy Commissioner for the year ended 30 June 2011 included on the Privacy Commissioner's website. The Privacy Commissioner's Board is responsible for the maintenance and integrity of the Privacy Commissioner's website. We have not been engaged to report on the integrity of the Privacy Commissioner's website. We accept no responsibility for any changes that may have occurred to the financial statements since they were initially presented on the website.

The audit report refers only to the financial statements named above. It does not provide an opinion on any other information which may have been hyperlinked to or from the financial statements. If readers of this report are concerned with the inherent risks arising from electronic data communication they should refer to the published hard copy of the audited financial statements and the related audit report dated 27 October 2011 to confirm the information included in the audited financial statements presented on this website.

Legislation in New Zealand governing the preparation and dissemination of financial information may differ from legislation in other jurisdictions.

STATEMENT OF OBJECTIVES AND SERVICE PERFORMANCE 2010/11

Output 1 – Compliance

Handle complaints of interference with privacy.

Participate in Human Rights Review Tribunal and Court cases as appropriate.

Monitor active information matching programmes.

Quantity	Estimation	Achieved
Number of complaints received.	800 – 1,000	968
Number of current complaints processed to completion or settled or discontinued.	800	999
Projected number of active information matching programmes monitored.	53	47
Participation in Human Rights Review Tribunal and Court cases.	6	3

Quality	Achievement
Complainants' and respondents' satisfaction with the complaints handling process rated as "satisfactory" or better in 80% of responses to a survey of complaints received and closed in the preceding period.	<p>Not achieved.</p> <p>Survey of both complainants and respondents conducted through out 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>Overall 77.5% of those who replied felt the process was satisfactory or better.</p>
Of the complaints processed, 30% are closed by settlement between the parties.	<p>Not achieved.</p> <p>28% of the complaints processed, were closed by settlement between the parties.</p> <p>The Office encourages complainants and respondents to reach settlement as a preferred outcome, but it relies on the willingness of the parties involved, it is not something for which the Office has direct control.</p>
On 90% of the complaints closed we demonstrate personal contact, either by phone or in person, with one or more of the parties.	<p>Achieved.</p> <p>90% of the complaints closed received personal contact, either by phone or in person, with one or more of the parties</p>

Quality	Achievement
External review is conducted of a sample of complaints investigations for their standard of the legal analysis, correctness of the legal conclusions, soundness of the investigative procedure and timeliness.	Achieved. External audit of 20 randomly selected complaint files. Overall the files collectively scored 91.5 out of a possible 100 points, an improvement on the previous year (90).
Provide all draft reports on operating information matching programmes to the relevant departments for comment before they are published in the Annual Report.	Achieved. Reports are submitted to relevant departments prior to publication in the annual report.

Timeliness	Achievement
80% of complaints are completed, settled or discontinued within 9 months of receipt.	Achieved. 91% of complaints were completed, settled or discontinued within 9 months of receipt. The timeliness standard was raised from the previous standard in 2010 year of 80-90% within 12 months.
Report on all operating information matching programmes in the Annual Report.	Achieved. A report on all authorised information matching programmes is provided in the Annual Report of the Office of the Privacy Commissioner.

Output 2 – Information and Outreach

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

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

Quantity	Achievement
Organise annual New Zealand Privacy Awareness Week as part of Asia-Pacific Privacy Awareness Week.	Achieved. Privacy Awareness Week ran from 1-7 May, in conjunction with other Asia-Pacific Privacy Authority members.

6: FINANCIAL & PERFORMANCE STATEMENTS

Quantity	Achievement
All media enquiries are recorded, logged and responded to within required deadlines.	Partly achieved. The Office responded to 212 media enquiries. The deadlines for a media enquiry will vary according to the individual requirements of the enquirer, for this reason the ability to provide a defined deadline for measurement is not possible.
Provide assistance to promote better privacy practice in the development of policy and legislation and administrative practices by government agencies.	Achieved. Apart from individual policy advice for different agencies, we also produced some specific tools this year. The "Getting started" guidance material is particularly targeted at policy advisers. Produced the health privacy toolkit. Produced Christchurch earthquake (Information Sharing) Code.
Provide an enquiries service including 0800 helpline and website access to information, supporting self-resolution of complaints.	Achieved. The Enquiries line is operated by two staff who fielded over 7000 calls and contacts during this financial year. The website contains a broad range of guidance material for users along with a series of Frequently Asked Questions (FAQ's) to assist self-resolution of complaints.
Preparation of practical guidance materials to assist public awareness and understanding of the Privacy Act.	Achieved. Health privacy toolkit (May 2011). Youth privacy kit launched (31 August 2010). Information on collection principles added to website.
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. Website performance reviewed during reporting year. Improved search functionality by adding advanced search feature. Added subscription feature so users can self-manage subscription to publications. The website is constantly maintained and new information is added within a week of becoming available (usually within 24 hours).

Activities	Estimation	Achieved
Education workshops delivered.	30	37
Presentations at conferences/seminars	15	44
Projected number of enquiries received and answered.	6,000	7,000
Case notes produced.	10	13
Media enquiries.	250	212

Quality	Achievement
Seek out and act on feedback obtained from stakeholders and the public.	Achieved. Example: peer review of guidance material, and offshore ICT survey.
Evaluations show that the expectations of 90% of attendees at workshops were either met or exceeded for quality of presentation and materials.	Achieved. 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 100% of instances.
Case notes are accepted and published by the Asia Pacific Privacy Authorities (APPA).	Achieved. Case notes are published and posted on the Asia Pacific Privacy Authorities (APPA) website. Case notes must comply with the citation standard as set by APPA before they may be posted on the website.
Website publications provide reliable and relevant information which is legally accurate and in plain English.	Achieved. Examples include public statements on various topics, reports to Parliament, and guidance material. Website review conducted during year which, among other matters, reviewed accuracy and relevance of site content.

Timeliness	Achievement
Current information is placed on the website within 5 working days of being made available.	Achieved. Information placed on website within 24 hours of being made available.
Response to 90% of enquiries within one working day.	Achieved. 92% of enquiries were responded to within one working day.

Output 3 – Policy and International

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, providing comment and other contributions as requested.	Achieved. Attended regular monthly meetings with the Law Commission. Provided submissions and comment as requested.
Issue the amendment to the Credit Reporting Privacy Code 2004;.	Achieved. Decision taken to complete in two amendments. Amendment No.4 issued in December 2010. Amendment No.5 released for public consultation in May 2011 but not issued by end of reporting year.
Provide practical advice to departments on privacy issues and fair information practices in proposed legislation and administrative proposals including additional support to agencies as they undertake privacy impact assessments.	Achieved. The Office responded to 79 new requests for advice from government departments, across a variety of issues.
Provide specialised assistance to government departments in accordance with agreed memoranda of understanding (currently the Department of Internal Affairs and Ministry of Health).	Achieved. Targets set out in the two work plans agreed with the Ministry of Health and the Department of Internal Affairs met, with minor exceptions involving two non-critical projects for the Ministry of Health. Progress with the work plan is monitored through quarterly progress reports and meetings with the Department or Ministry involved.
Provide assistance to improve whole-of-government compliance with information matching controls to support the efficient delivery of front line services.	Achieved. Completed 1 report under s106 of the Privacy Act. 4 new information matches reviewed by the Commissioner. 47 Active matches monitored.

Quantity	Achievement
Participate in international forums.	Achieved. Participated in OECD Conference, APPA Forum (2 meetings), International Conference of Data Protection and Privacy Commissioners.

Quantity	Achievement
Contribute to international initiatives to facilitate cross-border co-operation in privacy standard setting and enforcement.	Achieved. Contributed to launch of APEC Cross-border Privacy Enforcement Arrangement (CPEA) in July 2010, became one of the first CPEA members, became CPEA co-Administrator to assist successful implementation. Cofounded with 12 other privacy enforcement authorities the Global Privacy Network (GPEN) in September 2010, became member of GPEN Participation Committee to assist successful implementation.

Quality	Achievement
The Amendment to the Credit Reporting Privacy Code 2004 will be the subject of discussion with stakeholders and a public submission process which includes a clear statement of purpose.	Achieved. Amendment No.4 preceded by discussions with stakeholders, including an external reference group, and full public submission process including meetings with submitters. Amendment No.5 initiated by written submission process followed by public hearings of submissions.
The Amendment to the Credit Reporting Privacy Code 2004 will be referred to the Regulations Review Committee of the House of Representatives.	Achieved. Amendment No.4 referred to Regulations Review Committee and presented to Parliament.
Assistance provided to government agencies presents a clear, concise and logical argument, and is supported by facts.	Achieved. Across the 69 activities during the year where effectiveness could be assessed, the Office's view resulted in some or substantive improvement in 40 cases. In the view of the Office no changes were required in a further 13 cases. This level of achievement requires that the standard be met as a minimum.
Respond to feedback obtained from recipients of policy advice.	Limited actionable feedback has been received from recipients of policy advice.

6: FINANCIAL & PERFORMANCE STATEMENTS

Timeliness	Achievement
<p>Amendment 5 of the Credit Reporting Privacy Code 2004 will be released and implemented before 30 June 2011.</p>	<p>Not achieved.</p> <p>Amendment No.4 released for public consultation and issued before 30 June 2011.</p> <p>Amendment No.5 released for public consultation prior to 30 June but not issued by that date. The decision was made that due to the significant changes contained in the new Code a process of wider consultation would be appropriate. In addition the Australian Federal Privacy Commissioner was in the process of a change to their credit requirements which needed to be reflected in the new Code. There was a delay in the introduction of these changes putting back the timetable for New Zealand.</p>
<p>Advice given to agencies by the agreed date so that it is useful to them.</p>	<p>Achieved.</p> <p>Timeframes consistently met, even when short notice provided by agency.</p>

STATEMENT OF ACCOUNTING POLICIES

FOR THE YEAR ENDED 30 JUNE 2011

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 2011, and were approved by the Commissioner on 27 October 2011. 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 a historical cost basis.

Functional and presentation currency

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

Significant accounting policies

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

Budget figures

The budget figures are those approved by the Privacy Commissioner at the beginning of the financial year.

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

Revenue

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

Revenue from the Crown

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

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

Other grants

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

Interest

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

Sale of publications

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

Rental income

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

Provision of services

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

Leases

Operating leases

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

Goods and Services Tax (GST)

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

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

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

Commitments and contingencies are disclosed exclusive of GST.

Income Tax

The Privacy Commissioner is a public authority for tax purposes and therefore exempt from income tax. Accordingly no provision has been made for income tax.

Cash and cash equivalents

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

Debtors and other receivables

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

Impairment of a receivable is established when there is objective evidence that the Privacy Commissioner will not be able to collect amounts due according to the original terms of the receivable. Significant financial difficulties of the debtor, probability that the debtor will enter into bankruptcy, and default in payments are considered indicators that the debtor is impaired. The amount of the impairment is the difference between the asset's carrying amount and the present value of estimated future cash flows, discounted using the original effective interest rate. The carrying amount of the asset is reduced through the use of an allowance account, and the amount of the loss

is recognised in the statement of comprehensive income. When the receivable is uncollectible, it is written off against the allowance account for receivables. Overdue receivables that have been renegotiated are reclassified as current (i.e. not past due).

Inventories

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

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

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

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

Property, plant and equipment

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

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

Revaluations

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

Depreciation

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

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

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

Additions

The cost of an item of property, plant and equipment is recognised as an asset only when it is probable that future economic benefits or service potential associated with the item will flow to the Privacy Commissioner and the cost of the item can be measured reliably.

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

Disposals

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

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

Subsequent costs

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

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

Intangible assets**Software acquisition**

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

Staff training costs are recognised as an expense when incurred.

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

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

Amortisation

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

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

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

Impairment of non-financial assets

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

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

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

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

Creditors and other payables

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

Employee entitlements

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

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

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

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

Superannuation schemes

Defined contribution schemes

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

Financial instruments

The Privacy Commissioner is party to financial instruments as part of its normal operations. These financial instruments include bank accounts, short-term deposits, debtors, and creditors. All financial instruments are recognised in the statement of financial position and all revenues and expenses in relation to financial instruments are recognised in the statement of comprehensive income.

Statement of cash flows

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

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

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

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

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

Critical accounting estimates and assumptions

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

Property, plant and equipment useful lives and residual value

At each balance date the Privacy Commissioner reviews the useful lives and residual

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

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

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

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

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

Critical judgements in applying the Privacy Commissioner's accounting policies

Management has exercised the following critical judgements in applying the Privacy Commissioner's accounting policies for the period ended 30 June 2011:

Leases classification

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

Non-government grants

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

Changes in accounting policies

There have been no changes in accounting policies during the financial year.

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

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

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

- NZ IFRS 9 Financial Instruments will eventually replace NZ IAS 39 Financial Instruments: Recognition and Measurement. NZ IAS 39 is being replaced through the following 3 main phases: Phase 1 Classification and Measurement, Phase 2 Impairment Methodology, and Phase 3 Hedge Accounting. Phase 1 has been completed and has been published in the new financial instrument standards NZ IFRS 9. NZ IFRS 9 uses a single approach to determine whether a financial asset is measured at amortised cost or fair value, replacing the many different rules in NZ IAS 39. The approach in NZ IFRS 9 is based on how an entity manages its financial assets (its business model) and the contractual cash flow characteristics of the financial assets. The financial liability requirements are the same as those of NZ IAS 39, except for when an entity elects to designate a financial liability at fair value through the surplus/deficit. The new standard is required to be adopted for the year ended 30 June 2014. The Privacy Commissioner has not yet assessed the effect of the new standard and expects it will not be early adopted.
- NZ IFRS 7 Financial Instruments: Disclosures – The effect of early adopting these amendments is the following information is no longer disclosed:
 - the carrying amount of financial assets that would otherwise be past due or impaired whose terms have been renegotiated; and
 - the maximum exposure to credit risk by class of financial instrument if the maximum credit risk exposure is best represented by their carrying amount.
- NZ IFRS 24 Related Party Disclosures (Revised 2009) – The effect of early adopting the revised NZ IAS 24 is:
 - more information is required to be disclosed about transactions between the Privacy Commissioner and entities controlled, jointly controlled, or significantly influenced by the Crown;
 - commitments with related parties require disclosure;
 - information is required to be disclosed about any related party transactions with Ministers of the Crown.

STATEMENT SPECIFYING COMPREHENSIVE INCOME

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

Specified comprehensive income	Target \$000	Achievement \$000
Operating Grant	3,148	3,148
Other Revenue	300	325
Total Revenue	3,448	3,473

Output operating performance

The Privacy Commissioner committed to provide three output classes in 2010/11 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	1,066	1,075
Information & 'Outreach'	931	911
Compliance	1,499	1,487
Total	3,496	3,473

STATEMENT OF COMPREHENSIVE INCOME

FOR THE YEAR ENDED 30 JUNE 2011

	Note	Actual 2011 \$000	Budget 2011 \$000	Actual 2010 \$000
Income				
Crown revenue	2	3,148	3,148	3,148
Other revenue/seminars	3	285	270	342
Interest income		40	30	35
Total income		3,473	3,448	3,525
Expenditure				
Promotion	4	38	53	97
Audit Fees		23	18	21
Depreciation and Amortisation	1, 10, 11	143	150	171
Rental Expense		398	403	371
Operating Expenses		430	391	480
Staff Expenses	5	2,441	2,481	2,483
Total Expenditure		3,473	3,496	3,623
Deficit		0	(48)	(98)
Other comprehensive income		-	-	-
Total Comprehensive Income		0	(48)	(98)

The accompanying notes form part of these financial statements.

Explanations for significant variances against budget are provided in note 1.

STATEMENT OF CHANGES IN EQUITY

FOR THE YEAR ENDED 30 JUNE 2011

	Note	Actual 2011 \$000	Budget 2011 \$000	Actual 2010 \$000
Public equity as at 1 July		528	601	626
Surplus/(deficit)		0	(47)	(98)
Other comprehensive income		-	-	-
Total comprehensive income		0	(47)	(98)
Public equity as at 30 June	6	528	554	528

The accompanying notes form part of these financial statements.

STATEMENT OF FINANCIAL POSITION

AS AT 30 JUNE 2011

	Note	Actual 2011 \$000	Budget 2011 \$000	Actual 2010 \$000
Public Equity				
General funds	6	528	554	528
Total public equity		528	554	528
Assets				
Current assets				
Cash and cash equivalents	7	606	411	465
Debtors and other Receivables	8	9	75	10
Prepayments	8	23	8	25
Inventory	9	21	4	10
Total current assets		659	498	510
Non-current assets				
Property, plant and equipment	10	224	281	292
Intangible assets	11	2	-	52
Total non-current assets		226	281	344
Total assets		885	779	854
Liabilities				
Current liabilities				
Creditors and other Payables	12	245	145	208
Employee entitlements	13	110	80	117
Total current liabilities		355	225	325
Total liabilities		355	225	325
NET ASSETS		528	554	528

The accompanying notes form part of these financial statements.

STATEMENT OF CASH FLOWS

FOR THE YEAR ENDED 30 JUNE 2011

	Note	Actual 2011 \$000	Budget 2011 \$000	Actual 2010 \$000
Cash Flows from operating activities				
Cash was provided from:				
Supply of outputs to the Crown		3,354	3,148	3,384
Revenues from services provided		65	271	120
Interest received		40	30	35
Cash was applied to:				
Payments to suppliers		888	864	994
Payments to employees		2,441	2,482	2,570
Net Goods and Services Tax		(27)	211	19
Net cash flows from operating activities	14	157	103	(42)
Cash Flows from Investing Activities				
Cash was provided from:				
Landlord's capital contribution		8	8	-
Cash was applied to:				
Purchase of Property Plant and equipment		(24)	150	(113)
Purchase of Intangible Assets			-	-
Net cash flows from investing activities		(16)	142	(113)
Net increase (decrease) in cash held		141	(40)	(155)
Plus opening cash		465	451	620
Closing cash balance		606	411	465
Cash and bank		606	411	465
Closing cash balance		606	411	465

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 notes form part of these financial statements.

STATEMENT OF COMMITMENTS

AS AT 30 JUNE 2011

	Actual 2011 \$000	Actual 2010 \$000
Operating lease commitments approved and contracted		
Non-cancellable operating lease commitments, payable		
The future aggregate minimum lease payments to be paid under non-cancellable leases are as follows:		
Not later than one year	355	381
Later than one year and not later than five years	891	1,212
Later than five years	-	109

Other non-cancellable contracts

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

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

Total future minimum sublease payment to be received under non-cancellable subleases for office space at the balance date are \$49,464 (2010: \$74,196)

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

Capital commitments

The Privacy Commissioner has no capital commitments for the year. (2010 \$nil)

STATEMENT OF CONTINGENT LIABILITIES

AS AT 30 JUNE 2011

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 (2010 : nil).

NOTES TO THE FINANCIAL STATEMENTS

FOR THE YEAR ENDED 30 JUNE 2011

Note 1: Total Comprehensive Income

	Actual 2011 \$000	Actual 2010 \$000
The total comprehensive income is after charging for:		
Fees paid to auditors		
External audit	-	-
Current Year	23	21
Prior Year	21	-
Depreciation:		
Furniture & Fittings	63	57
Computer Equipment	26	31
Office Equipment	4	12
Total Depreciation for the year	93	100
Amortisation of Intangibles	50	71
Rental expense on operating leases	398	371

Major budget variation

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

Statement of Comprehensive Income

Staff expenses

Lower than budgeted due to difficulties in finding suitable applicants for a senior staff position. The delay in filling the position providing savings in personnel expenditure. The position was subsequently filled.

Operating expenses

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

Computer maintenance

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

Litigation

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

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 (2010 nil).

Note 3: Other revenue

	Actual 2011 \$000	Actual 2010 \$000
Other grants received	206	236
Rental income from property sub-leases	25	19
Privacy Forum	-	41
Seminars & Workshops	35	34
Sponsorship*	-	-
Other	19	12
Total other revenue	285	342

Note 4: Promotion expenses

	Actual 2011 \$000	Actual 2010 \$000
Website development expenses	10	19
Inventories consumed	7	26
Other marketing expenses	21	52
Total marketing expenses	38	97

Note 5: Staff expenses

	Actual 2011 \$000	Actual 2010 \$000
Salaries and wages	2,288	2,279
Employer contributions to defined contribution plans	35	34
Other Staff expenses	46	126
Increase/(decrease) in employee entitlements (note 13)	(7)	(70)
Other contracted services	79	114
Total Staff Expenses	2,441	2,483

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

Note 6: General funds

	Actual 2011 \$000	Actual 2010 \$000
Opening balance	528	626
Net (deficit) / surplus	0	(98)
Closing balance	528	528

Note 7: Cash and cash equivalents

	Actual 2011 \$000	Actual 2010 \$000
Cash on hand and at bank	46	47
Cash equivalents – term deposits	560	418
Total cash and cash equivalents	606	465

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 2011 \$000	Actual 2010 \$000
Trade debtors	9	10
Prepayments	23	25
Total	32	35

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 (2010 \$NIL).

Impairment

The aging profile of receivables at year end is detailed below:

Aging analysis:	2011
Not past due	7,316
Past due 1-30 days	1,410
Past due 31-60 days	62
Past due 61-90 days	170
Past due >91 days	-
Total debtors and other receivables	8,958

As at 30 June 2011 the Privacy Commissioner no debtors have been identified as insolvent. (2010 \$NIL).

Note 9: Inventories

	Actual 2011 \$000	Actual 2010 \$000
Publications held for sale	21	10

The carrying amount of inventories held for distribution that are measured at current replacement cost as at 30 June 2011 amounted to \$NIL (2010 \$NIL).

There have been no write-down of inventories held for distribution or reversals of write-downs (2010 \$NIL).

No inventories are pledged as security for liabilities (2010 \$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
Cost				
Balance at 1 July 2009	481	159	114	754
Additions	80	32	2	114
Balance at 30 June 2010	561	191	116	868
Balance at 1 July 2010	561	191	116	868
Additions	2	23	-	25
Disposals	(148)	-	-	(148)
Balance at 30 June 2011	415	214	116	745
Accumulated depreciation and impairment losses				
Balance at 1 July 2009	277	104	94	475
Depreciation expense	57	31	12	100
Balance at 30 June 2010	334	134	107	575
Balance at 1 July 2010	334	134	107	575
Depreciation expense	63	26	4	93
Disposals	(148)	-	-	(148)
Balance at 30 June 2011	249	160	111	520
Carrying amounts				
At 30 June and 1 July 2010	227	56	9	292
At 30 June 2011	166	53	5	224

Note 11: Intangible assets

Movements for each class of intangible asset are as follows:

	Acquired software \$000
Cost	
Balance at 1 July 2009	283
Additions	-
Balance at 30 June 2010	283
Balance at 1 July 2010	283
Additions	-
Balance at 30 June 2011	283
Accumulated amortisation and impairment losses	
Balance at 1 July 2009	160
Amortisation expense	71
Balance at 30 June 2010	231
Balance at 1 July 2010	231
Amortisation expense	50
Balance at 30 June 2011	281
Carrying amounts	
At 1 July 2009	123
At 30 June and 1 July 2010	52
At 30 June 2011	2

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 2011 \$000	Actual 2010 \$000
Creditors	67	43
Income in advance	0	0
Accrued expenses	80	94
Other payables	98	71
Total creditors and other payables	245	208

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 2011 \$000	Actual 2010 \$000
Current employee entitlements are represented by:		
Accrued salaries and wages	7	0
Annual leave	103	117
Total current portion	110	117
Current	110	117
Non-current	-	-
Total employee entitlements	110	117

Note 14: Reconciliation of total comprehensive income from operations with the net cashflows from operating activities

	Actual 2011 \$000	Actual 2010 \$000
Total comprehensive income	0	(98)
Add/(less) non-cash items:		
Depreciation and Amortisation	143	171
Other non Cash Items	-	-
Total non-cash items	143	171
Add/(less) movements in working capital items:		
(Increase)/Decrease in receivables	1	134
(Increase)/Decrease in prepayments	2	(17)
(Increase)/Decrease in inventory	(11)	-
Increase/(Decrease)in payables	37	(44)
Increase/(Decrease)in employee entitlements	(7)	(70)
Increase/(Decrease) in Income in Advance	-	(120)
Working capital movements - net	22	(119)
Add/(less) items classified as investing activities:		
Landlord's capital contribution	(8)	-
Total investing activity items	(8)	-
Net cash flow from operating activities	157	(42)

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. The Office paid the Trust \$200 for membership fees there were no other transactions with this Trust during the current financial year. (In 2010 there were no transactions with this Trust during the financial year)

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 2011 \$000	Actual 2010 \$000
Total Salaries and other short-term employee benefits	859	832

Key management personnel include all Senior Management Team members, the Privacy Commissioner who together comprise the Leadership Team.

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 2011 \$000	Actual 2010 \$000
\$100,000 - \$109,999		1
\$110,000 - \$119,999		
\$120,000 - \$129,999		1
\$130,000 - \$139,999	2	1
\$140,000 - \$149,999	1	1
\$150,000 - \$159,999		
\$160,000 - \$169,999	1	1
\$260,000 - \$269,999		1
\$270,000 - \$279,999	1	

The 2010 split has been restated in line with CEAs152(1)(c)

Note 17: Commissioners' total remuneration

In accordance with the disclosure requirements of Section 152 (1)(a) of the Crown Entities Act 2004, the total remuneration includes all benefits paid during the period 1 July 2010 to 30 June 2011.

Name	Position	Amount 2011	Amount 2010
Marie Shroff	Privacy Commissioner	\$273,527	\$263,502

Note 18: Cessation payments

No redundancy payments were made in the year. (2010 : NIL)

Note 19: Indemnity insurance

The Privacy Commissioner's insurance policy covers public liability of \$10million and professional indemnity insurance of \$1,000,000.

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**21A Financial instrument categories**

The accounting policies for financial instruments have been applied to the line items below:

	Actual 2011 \$000	Actual 2010 \$000
FINANCIAL ASSETS		
Loans and Receivables		
Cash and cash equivalents	606	465
Debtors and other receivables	9	10
<i>Total loans and receivables</i>	615	475
FINANCIAL LIABILITIES		
Financial liabilities at amortised cost		
Creditors and other payables	245	208
<i>Total financial liabilities at amortised cost</i>	245	208

21B Financial instruments risk

The Privacy Commissioner has a series of policies providing risk management for interest rates, operating and capital expenditures denominated in a foreign currency, and the concentration of credit. The Privacy Commissioner is risk averse and seeks to minimise its exposure from its treasury activities. Its policies do not allow any transactions which are speculative in nature to be entered into.

Credit risk

Credit risk is the risk that a third party will default on its obligation to the Privacy Commissioner, causing the Privacy Commissioner to incur a loss. Financial instruments which potentially subject the Office to risk consist principally of cash, short term investments, and trade receivables.

The Privacy Commissioner has a minimal credit risk in its holdings of various financial instruments. These instruments include cash, bank deposits.

The Privacy Commissioner places its investments with institutions that have a high credit

rating. The Privacy Commissioner believes that these policies reduce the risk of any loss which could arise from its investment activities. The Privacy Commissioner does not require any collateral or security to support financial instruments.

The institution's credit ratings are:

Rating Agency	Current credit rating	Qualification
Standard & Poor's	AA	Outlook Stable
Moody's Investors Service	Aa3	Outlook Stable
Fitch Ratings	AA-	Outlook Positive

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 2011 (2010: 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	Fixed maturity dates – less than 1 year	Non interest bearing
2011 Financial assets	%	NZ \$000	NZ \$000	NZ \$000
Cash and cash equivalents	-	606	-	-
	-	606	-	-
2010 Financial Assets				
Cash and cash equivalents	3	465	-	-
	3	465	-	-

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 2011 NZ \$000	Net surplus 2010 NZ \$000
Cash and cash equivalents +100 bps	3.25	4.65
Cash and cash equivalents – 100 bps	(3.25)	(4.65)

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