

Privacy Commissioner

Annual Report 2012



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

© 2012 The Privacy Commissioner

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

ANNUAL REPORT OF THE PRIVACY COMMISSIONER

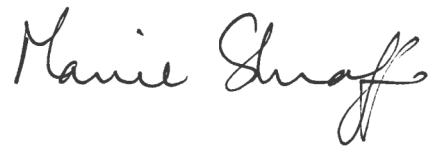
For the year ended 30 June 2012

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

November 2012

THE MINISTER OF JUSTICE

I tender my report as Privacy Commissioner
for the year ended 30 June 2012.

A handwritten signature in black ink, reading "Marie Shroff". The signature is written in a cursive style with a large, stylized initial 'M'.

Marie Shroff
Privacy Commissioner

CONTENTS

1: KEY POINTS	9
2: INTRODUCTION.....	13
3. REPORT ON ACTIVITIES.....	19
International activities	19
Highlights	20
Information services.....	20
Enquiries	20
Training and education	21
Privacy Awareness Week (29 April – 5 May 2012)	21
The UMR public opinion survey	22
Advice cards for seniors	22
Other outreach	23
Media	23
Social media	24
Complaints and access reviews.....	24
The complaints process	24
Settlement.....	25
Personal contact.....	26
Complaints received	26
Agency types.....	26
Age of complaints	27
Top respondent agencies	27
External audit	29
Litigation.....	30
Human Rights Review Tribunal.....	30
Commissioner initiated inquiries.....	31
Section 54 authorisations.....	31
Digital Switchover.....	31
Veda Advantage	32
Ministry of Education	32
Policy	32
Legislation and other government policy.....	32
Health advice.....	33
Technology advice	33
Information matching.....	34
Codes of practice	34
Credit Reporting Privacy Code	34
Proposed Civil Defence National Emergencies (Information Sharing) Code	35
Consultations with the Ombudsmen.....	36

CONTENTS

4: OFFICE OF THE PRIVACY COMMISSIONER	39
Independence and competing interests	39
Reporting	39
Staff	39
Equal employment opportunities.....	40
5. INFORMATION MATCHING	43
Information matching and privacy – an introduction.....	43
Glossary	44
The year in information matching	45
Outreach	45
Changes in authorised and operating programmes.....	46
Periodic review (s.106) of information matching programmes	46
Online transfer approvals	46
Programme reports.....	48
1. Corrections/ACC Prisoners Programme	48
2. IR/ACC Levies and Compensation Programme	49
3. Citizenship/BDM Citizenship by Birth Processing Programme.....	49
4. BDM/DIA(C) Citizenship Application Processing Programme	50
5. BDM/DIA(P) Passport Eligibility Programme	51
6. Citizenship/DIA(P) Passport Eligibility Programme.....	51
7. Citizenship/EEC Unenrolled Voters Programme	52
8. DIA (Passports)/EEC Unenrolled Voters Programme.....	53
9. INZ/EEC Unqualified Voters Programme	53
10. MoT/EEC Unenrolled Voters Programme.....	54
11. MSD/EEC Unenrolled Voters Programme	55
12. NZTA/EEC Unenrolled Voters Programme	55
13. BDM(Deaths)/GSF Eligibility Programme.....	56
14. BDM(Deaths)/INZ Deceased Temporary Visa Holders Programme.....	56
15. Citizenship/INZ Entitlement to Reside Programme.....	57
16. Corrections/INZ Prisoners Programme	57
17. Customs/IR Child Support Alerts Programme	58
18. Customs/IR Student Loan Interest Programme	59
19. MSD/IR Working For Families Tax Credits Administration Programme.....	60
20. MSD/IR Working for Families Tax Credits Double Payment Programme.....	60
21. Customs/Justice Fines Defaulters Alerts Programme	61
22. INZ/Justice Fines Defaulters Tracing Programme	62
23. IR/Justice Fines Defaulters Tracing Programme	63
24. MSD/Justice Fines Defaulters Tracing Programme.....	65
25. Customs/MED Motor Vehicle Traders Importers Programme	66

CONTENTS

26. MOT/MED Motor Vehicle Traders Sellers Programme	67
27. BDM(Births)/Ministry of Health NHI and Mortality Register Programme	68
28. BDM(Deaths)/Ministry of Health NHI and Mortality Register Programme	68
29. INZ/MoH Publicly Funded Health Eligibility Programme.....	69
30. ACC/MSD Benefit Eligibility Programme	69
31. BDM/MSD Identity Verification Programme	71
32. BDM(Deaths)/MSD Deceased Persons Programme	72
33. BDM(Marriages)/MSD Married Persons Programme	72
34. Centrelink/MSD Change in Circumstances Programme	73
35. Centrelink/MSD Periods of Residence Programme	74
36. Corrections/MSD Prisoners Programme.....	74
37. Customs/MSD Arrivals & Departures Programme	76
38. Customs/MSD Periods of Residence Programme	77
39. Educational Institutions/MSD (StudyLink) Loans & Allowances Programme	78
40. HNZ/MSD Benefit Eligibility Programme.....	78
41. IR/MSD Commencement/Cessation Benefits Programme.....	79
42. IRD/MSD Commencement/Cessation Students Programme.....	80
43. IR/MSD Community Services Card Programme.....	81
44. IR/MSD (Netherlands) Tax Information Programme	82
45. MoE/MSD (StudyLink) Results of Study Programme	82
46. Netherlands/MSD Change in Circumstances Programme	83
47. Netherlands/MSD General Adjustment Programme	84
48. BDM(Deaths)/NPF Eligibility Programme	84
49. BDM (Deaths)/NZTA Deceased Driver Licence Holders Programme	85
50. MoE/Teachers Council Registration Programme	86
6: FINANCIAL & PERFORMANCE STATEMENTS	89
Statement of responsibility	89
Audit Report	90
Statement of objectives and service performance 2011/12	92
Statement specifying comprehensive income	92
Statement of objectives and service performance for the year ended 30 June 2012.....	93
Statement of accounting policies for the year ended 30 June 2012	99
Statement of comprehensive income for the year ended 30 June 2012.....	109
Statement of changes in equity for the year ended 30 June 2012	109
Statement of financial position as at 30 June 2012	110
Statement of cash flows for the year ended 30 June 2012.....	111
Statement of commitments as at 30 June 2012.....	112
Statement of contingent liabilities as at 30 June 2012	112
Notes to the financial statements for the year ended 30 June 2012.....	113

CONTENTS

Section 3 Tables

Table 1: Complaints received and closed 2007-2012	24
Table 2: Settlement outcomes 2011/12.....	26
Table 3: Act/Code – breakdown of complaints received 2011/12.....	26
Table 4: Complaints received by agency type 2011/12	27
Table 5: Complaints received and closed for top respondent agencies 2011/12.....	28
Table 6: Outcomes for top respondents agencies 2011/12.....	29
Table 7: Referrals, tribunal cases and outcomes 2006-2012	30

Section 4 Tables

Table 8: Workplace gender profile 2011/12	40
Table 9: Workplace ethnic profile 2011/12.....	41

Section 5 Tables

Table 10: First time online transfers approvals 2011/12	47
Table 11: Renewed approvals 2011/12.....	47

Figures

Figure 1: Age of closed complaints 2011/12	27
Figure 2: Active authorised information matching programmes 2011/12.....	45
Figure 3: Authorised, operating and inoperative information matching programmes 2003-2012..	46

1: KEY POINTS

1: KEY POINTS

Information and communications

- We received over 8,000 (8,465) enquiries from members of the public and organisations seeking advice on privacy matters.
- This year we had 295 media enquiries. The ACC privacy breach accounted for a high number of calls – around 70. The other enquiries have most frequently focused on technology-related subjects. CCTV, cyberbullying and other social media topics, Google's new privacy policies, phone hacking, and automatic number plate recognition were among the topics raised.
- We released the results of our latest UMR public opinion survey in May. General concern about privacy has risen sharply in the last decade (up to 67%, from 47% in 2001). More specifically, the public expects businesses and government agencies to be held accountable for privacy breaches.
- This year's Privacy Awareness Week, run with our partners from the Asia Pacific Privacy Authorities (APPA), included a one-day privacy forum in Wellington on the theme of "Think Big? Privacy in the Age of Big Data", which attracted 250 participants including speakers from New Zealand and overseas. APPA produced a one-stop list of key resources with advice for young people, parents and teachers.
- We launched new advice cards for seniors on the five topics that they saw as most important: financial privacy, scams, health information, business use of information, and keeping safe online. The development, production and distribution of the cards were supported by Neighbourhood Support and the Office for Senior Citizens.
- The Office started a Facebook page (<http://www.facebook.com/PrivacyNZ>) and a Twitter account (<https://twitter.com/NZPrivacy>) in early May as a new way of providing information to people.
- The Office delivered 46 workshops and seminars to members of the public and stakeholder groups. The Commissioner and staff also gave 47 presentations, such as to health and business groups, both in New Zealand and overseas.

Investigations

- We received 1,142 complaints, an increase on last year's 968.
- 30% 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.

- 95% of complaints are under nine months of age, with 83% closed within six months of receipt.

Policy and technology

- We monitored 50 active government information matching programmes this year, 33 of which use online data transfers.
- The Office provided advice on 57 agency files. We also contributed to major legislative projects including the Electronic Identity Verification Bill, Social Security (Youth Support and Work Focus) Amendment Act 2012, Privacy (Information Sharing) Bill, Victims of Crime Reform Bill and Land Transport Management Amendment Bill.
- We continued to provide advice to the National Health IT Board on electronic health records.
- Cloud computing has been one focus of our technology work. We have supported industry efforts to develop a code of practice for cloud computing providers, and have created privacy guidelines for small and medium sized businesses that are considering using cloud computing services.
- The Privacy Commissioner amended the Credit Reporting Privacy Code to enable New Zealand to move to more positive credit reporting. The Code was amended in two stages, involving public submissions for both stages. Amendment No. 4 was issued in December 2010 and Amendment No. 5 was issued in September 2011, with both coming into force in April 2012.
- We publicly notified the proposed Civil Defence National Emergencies (Information Sharing) Code in April, and sought public submissions. After issuing the Christchurch Earthquake (Information Sharing) Code immediately after the 22 February 2011 earthquake, we decided it would be useful to have a similar code in place in case New Zealand was ever again faced with a national emergency. The submission process closed in late May and submissions were still being considered at the end of June 2012.

International

- The Office continued its expert contribution to the OECD review of the 1980 Privacy Guidelines, including a presentation to an OECD conference in November.
- We pursued our efforts to secure a finding from the EU that New Zealand offers an 'adequate standard of data protection', with MFAT assistance.
- We continued to help lead the Global Privacy Enforcement Network (GPEN) through participation on the GPEN Committee. We have taken a lead in encouraging GPEN to coordinate multilateral cross-border investigations.

1: KEY POINTS

2: INTRODUCTION

2: INTRODUCTION

Some headlines from our year

ACC Inquiry

The Accident Compensation Corporation (ACC) data breach in March 2012, involving more than 6,500 clients, may prove a sort of watershed for the public sector. The effect has been to identify weaknesses at a systemic and governance level and there are salutary lessons to be learned. Recent comments by the State Services Commissioner, Iain Rennie, call the ACC inquiry report a 'dramatic reminder' and he goes on to suggest a state-sector wide stocktake.

The inquiry highlighted that data management needs to be thought of as an integral part of serving the public, and as a wider 'risk management' strategy. It is evident that the way personal information is handled can affect an organisation from top to bottom, and that is particularly so if its core business is holding and processing personal information.

The competitive driver in the private sector gives businesses a reality check: breaches of privacy lead to loss of customers. So there are some immediate – financial – incentives to get things right. The same driver does not exist in the public sector. Of course, the damage to public trust from privacy breaches is self-evident, and everyone is aware that public trust is essential for government agencies to be able to work effectively and efficiently. But 'trust' and 'efficiency' are relatively fuzzy concepts, that can be overlooked (albeit at the agency's peril) in the wider scheme of everyday government work. To get it right, the public sector needs to focus on privacy much more deliberately than it has yet done. As the ACC review shows, key areas for development include leadership, culture, personal information governance and risk management, and creating comprehensive privacy strategies to handle personal information throughout the agency.

New Zealanders are entitled to expect that our government agencies will handle their personal information safely and with respect.

Credit reporting code

Amendment 7 to the Credit Reporting Privacy Code, permitting more comprehensive credit reporting, came into effect in April 2012. Credit reporting is an area where there are strong interests both in ensuring the supply of sufficient information for the credit industry to operate and make sound decisions, while also ensuring adequate protection of each person's financial information. Accuracy of information is critical. There are multiple interests and commercial drivers to balance.

The decision to allow “positive” (or more comprehensive) credit reporting was not an easy decision for us. Arguments that positive credit reporting would help to provide a framework for a more responsible lending environment were ultimately persuasive.

Strong privacy protections have been built in to the new regime, and a code of consumer rights has been issued in 12 languages.

Credit reporting is an area that requires active and ongoing management to ensure that privacy and public interests are being served, because of its complexity, and because of the high stakes involved for individuals.

Businesses moving forward

Globally, regulators are taking a stronger line with companies. This trend is most evident in recent enforcement measures in the United States, for instance with the Federal Trade Commission’s settlements with Facebook and Google. There are also European Union proposals to tighten privacy regulation in the EU, including increasing fines for errant companies.

The move to greater cross-border enforcement and co-ordination is also gaining impetus, and our office has continued to play a significant role. The importance of this for economic growth is obvious. For instance, the World Economic Forum refers to the evidence of an emerging asset class of personal data, but also goes on to note the lack of rules, norms and frameworks that, by contrast, exist for other types of assets.¹ We may have the valued goods in the form of personal data – and the means of distribution through online networks – but we have sometimes lacked cross- border enforcement mechanisms and regulatory solutions for when things go wrong.

Many New Zealand companies are able and willing to handle personal information well, and we assist them to do so where we can. However, overall, the customer is still too often placed in the unfavourable position of having to bear the risk of transacting. Customers are becoming more resentful of bearing those risks and are demanding that companies be properly accountable for their actions. It is clear that people believe regulators should have – and use – the ability to call agencies to heel. For instance in our public opinion survey earlier this year, 97% of respondents said that the Privacy Commissioner should have the power to order an agency to comply with the law, and 88% said they wanted businesses punished if they misuse people’s personal information. The survey also illustrated a strong sense of disquiet about what personal information is used for and how it is handled.

There is a growing recognition that personal information can take on a life of its own in the wrong hands. Consumers’ confidence in how their information is

¹ World Economic Forum “Rethinking Personal Data: Strengthening Trust”, May 2012, p7.

managed has a direct impact on profits, and on the opportunities for New Zealand Inc. There are real risks that customers will disengage unless they are sure that there are sufficient checks and balances to make sure that their information is properly protected.

Competition has a major part to play – businesses that are found to abuse privacy will lose customers to more responsible players. However, the law also has a role and we are actively participating in moves to ensure customers can be better protected both at home and abroad.

Cloud computing guidance

A common theme for us for several years has been the focus on technology developments that provide both opportunities for and challenges to business and government. Handling personal information correctly is a key to unlocking the potential that new technologies have to offer, as well as to getting new and better uses from old technologies.

A major focus of this year for us and many others has been cloud computing. We have provided advice and support to the Institute of IT Professionals (formerly the Computer Society) while it has been working to draft a code of practice for cloud computing. The New Zealand Cloud Computing Code of Practice was released in draft at the Cloud Summit in May 2012.²

We have also been working on targeted cloud computing guidance for SMEs and expect to be able to make this guide freely available online shortly.

Privacy law reforms

The Privacy (Information Sharing) Bill received its first reading in February 2012, and the select committee reported back in June 2012. The Bill proposes to allow information sharing agreements within the public sector and also between public and private sectors. Expansion of information sharing raises potential privacy concerns and we have voiced our support of the safeguards that have been placed in the bill.³

The Information Sharing Bill forms only one part of the Law Commission's recommendations for privacy law change detailed in its comprehensive Review of Privacy.⁴ The Commission's final report was released in August 2011.

In March 2012, the Government provided a short response to the other privacy law recommendations made by the Law Commission.⁵ The principles-based approach of the Privacy Act will be retained, and the recommendation that there be a new Privacy Act has been accepted. A more detailed Government

² <http://www.nzcloudcode.org.nz/2012/05/cloud-computing-code-of-practice-released-at-cloud-summit/>

³ <http://privacy.org.nz/privacy-commissioner-supports-safeguards-in-information-sharing-bill-media-release/>

⁴ <http://www.lawcom.govt.nz/project/review-privacy>

⁵ <http://www.justice.govt.nz/publications/global-publications/g/government-response-privacy>

2: INTRODUCTION

response is still to come that will provide details of which Law Commission's recommendations have been accepted.

There is an undoubted need for the law to be updated to enable it to respond to modern problems. For example, because personal details can so easily be misused when data ends up in the wrong hands, people need to be told if there is a major data breach that could cause them harm. They should be provided with ability to protect themselves, such as cancelling a credit card before they, or the bank, incur financial loss. At the moment, however, there is no law requiring that affected individuals should be told about breaches.

In our view, the Law Commission's recommendations form a sensible, balanced and practical package of reforms that will facilitate good business and good government, and give New Zealanders greater confidence that their personal information will be adequately protected. We look forward to the government's more detailed response to those reform proposals.

3. REPORT ON ACTIVITIES

3. REPORT ON ACTIVITIES

International activities

There is an international dimension to many aspects of information privacy. Most significant is the cross-border transfer of personal information that is now so much an ordinary daily feature of business and personal life. In addition to changes in business processes, such as outsourcing and off-shoring, individuals have been empowered to be publishers and not merely consumers of content. It is now routine for individuals to publish information about themselves and others, literally to the world – something that would have been beyond most people's imagination 20 years ago.

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

- international collaboration can lead to common standards to facilitate business transactions across borders in ways that protect the interests of individuals.
- a company's actions in one country can affect the citizens in another. For instance, in the event of a security breach, we may need to seek the cooperation of enforcement authorities in other countries.
- other countries may encounter privacy challenges before they affect New Zealand. So collaboration with counterpart authorities can lead to enhanced problem solving, creative policy solutions and more effective regulation.

The office engages in a variety of forums, the principal ones being:

- Asia Pacific Privacy Authorities (APPA) forum: meets twice a year and involves commissioners from Australia, Canada, Hong Kong, Korea, Macau, 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 each year and undertakes inter-sessional work through working groups.
- APEC: the Data Privacy Subgroup (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 2011/12 were:

- OECD: we continued our contribution to the OECD Review of the 1980 Privacy Guidelines, including a presentation to an OECD conference in November 2011 and detailed input into the work of a Privacy Volunteer Group, including drafting revised Guidelines.
- European Union: we assisted MFAT in ensuring further progress was made towards securing a finding from the EU that New Zealand offers an 'adequate standard of data protection'.
- Asia Pacific Privacy Authorities Forum: we participated in APPA meetings in Melbourne and Hong Kong.
- Global Privacy Enforcement Network: we continued to help lead the network through participation on the GPEN Committee and by helping to arrange a meeting in Mexico. We have taken a lead in encouraging GPEN to coordinate multilateral cross-border investigations.
- APEC Cross-border Privacy Enforcement Arrangement: we continued as a CPEA administrator. This arrangement now connects 21 privacy enforcement authorities in seven APEC countries.
- International Conference of Data Protection and Privacy Commissioners: the Privacy Commissioner gave a presentation to the 33rd Annual Conference. The Conference adopted a resolution that we proposed on data protection in major natural disasters. The resolution drew upon lessons learnt from the Christchurch earthquake, and elsewhere. We joined a working group established by the conference on cross-border enforcement cooperation.

Information services

Enquiries

We received nearly 8,500 individual contacts through our enquiries services – up from 7,000 the year before. This is a substantial increase, even allowing for the fact that a large number of calls (around 380) were about the ACC privacy breach.

The service operates an 0800 phone line and an email address. As in past years about 80% of the enquiries are received by telephone. Email contact continues to increase, however, with around 20% of enquiries now being through email.

Nearly a third of all enquiries are about disclosure or use of personal information. The next largest area is about gaining access to information (around a fifth of all enquiries).

Most people who contact us are calling in their individual capacity (around 75%)

but small business and the health sector also use the service, contributing to about 15% of enquiries. We also received 162 calls from lawyers and law firms.

Training and education

This year was busier than the previous year. We undertook 48 workshops and seminars in Auckland, Tauranga, New Plymouth, Palmerston North, Wellington and Christchurch. As in previous years there is a high demand from the health sector with nearly 25% of the workshops being for health agencies.

Feedback from all sessions shows that attendees are very satisfied with the training and that they find the content and trainers of a high calibre.

Privacy Awareness Week (29 April – 5 May 2012)

Privacy Awareness Week is an international event organised by the Asia-Pacific Privacy Authorities forum (APPA). It is held during the first week in May in New Zealand, most Australian jurisdictions, Hong Kong, Macao, South Korea, Canada, Mexico and the United States.

This year, the APPA jurisdictions joined together to produce a one-stop list of key resources with advice for young people, parents and teachers. The list is available in several languages at <http://www.privacyawarenessweek.org/youth.html>.

In New Zealand, our Office's main event was a one-day privacy forum in Wellington on the theme of "Think big? Privacy in the age of big data". The forum was sold out, with around 250 participants including some excellent speakers from New Zealand and overseas. The programme included topics such as managing privacy in the arena of cloud computing; online tracking; privacy enhancing technologies; surveillance in public places; government information sharing; and regional shared healthcare. Some of the presentations are available on our Facebook page: <http://www.facebook.com/PrivacyNZ> and on YouTube (search under "Privacy in the Age of Big Data Forum").

Our other activities included:

- Releasing our UMR public opinion survey (discussed in more detail below)
- Publishing a new poster "Take the time to know your privacy principles"
- Organising a focus group of primary school teachers to discuss what resources and information are needed in primary schools (this is a continuing joint project with NetSafe, sponsored by UNESCO).

Many other agencies also undertook their own activities during Privacy Awareness Week, including various government departments, banks, universities and community organisations. In particular, the week featured the highly successful two-day Identity Conference, organised by Victoria University of Wellington and the Department of Internal Affairs, with support from our office.

The UMR public opinion survey

We released the results of our latest UMR public opinion survey in May. We run the survey every two years or so, which gives us valuable insights into trends in attitudes to privacy within the community.

General concern about privacy has risen sharply in the last decade (up to 67%, from 47% in 2001). More specifically, the public expects businesses and government agencies to be held accountable for privacy breaches. For instance:

- 88% of respondents said they wanted businesses punished if they misused personal information
- 97% of respondents said the Privacy Commissioner should have the power to order a company to stop breaching the Privacy Act
- 82% of respondents were worried about government agencies silently sharing their personal information
- Trust in government (68%) and business (65%) remains high but a relatively high proportion of the public remain neutral (22% about business and 17% about government)
- Discomfort with personal information handling by government and business continues to track at a high level (80 – 90%)

The digital environment is driving many of these concerns. While people recognise the benefits that technologies such as social networking can bring, they are concerned about issues such as online tracking (63%); targeted advertising (56%); what children put online about themselves (84%); and holding personal information offshore (56%, with another 22% neutral).

Seventy four percent of people have changed their privacy settings on Facebook. This shows that many people do care about their privacy on social networks and are making a serious attempt to control who is seeing their personal information. But 54% of people still consider that Facebook is a private space, including people who have made no attempt to change their privacy settings. There is a real risk that these people may have a false sense of security, leading them to post more sensitive information than they might otherwise do. For example, people are often not aware that their social media contacts can and do put information out in the open by re-sharing it, or that the social network providers themselves will almost certainly mine the information that users post.

Advice cards for seniors

With support from Neighbourhood Support and the Office for Senior Citizens, the Office produced advice cards aimed at seniors and the wider community. The cards were launched in September 2011 by Dame Catherine Tizard, and Wellington Mayor Celia Wade-Brown hosted the event.

The cards were the result of a focus group of senior citizens and people who work with senior citizens. The group told us that the aspects of privacy that most concerned older people were financial privacy, scams, health information, business use of information and keeping safe online. They told us what tips might best help those people and what forms of guidance material would be most useful. The result is this set of five cards, one on each of the key topics. They are proving useful for people of all ages in our communities.

The cards have been distributed nationwide through community and key organisations for older people and can also be ordered or downloaded from our website.

Other outreach

The Commissioner and her senior staff have given 47 speeches and presentations during the year on a wide range of topics and for a wide variety of audiences. Topics have included:

- Technology and business challenges for privacy
- Law Commission review – implications for auditors
- Privacy and legal limitations in the private investigations field
- Cloud computing
- Global Enforcement Coordination
- Human rights law and privacy
- Health information privacy and Law Commission recommendations
- Cross-Border Privacy Rules: implementing shared privacy values
- Public attitudes to privacy in the age of big data
- Privacy and Social Media: Get it right before you get it wrong.

Media

We had a near-record number of media enquiries this year (295). The only year in which we have had more was 2009/10 (323). Last year, we had a more normal number of 212.

Unsurprisingly, the ACC privacy breach accounted for a high number of media calls – around 70. This was the most we have ever had on a single topic. The media interest in ACC included periods of very high activity, particularly in the initial few weeks after the breach became public.

The challenges for us were significant, since we do not have any full time communications staff. Instead, we share media phone duties and have a team approach to other communications activities. The approach works well, as we each contribute different skills (including legal and technical knowledge). We are

also confident that we generally managed the high media workload successfully and in a helpful manner for our callers. However, this year it meant that we had to divert staff time away from other communications projects. For example we have had to delay our guidance for small and medium businesses about cloud computing.

As with previous years, the remaining enquiries have most frequently been focused on technology-related subjects. Among the topics raised were CCTV, cyberbullying and other social media topics, Google's new privacy policies, phone hacking, and automatic number plate recognition.

Social media

We started a Facebook page (<http://www.facebook.com/PrivacyNZ>) and a Twitter account (@NZPrivacy) in early May, as a new way of providing information. For example, our Facebook page enables us to use video, linked from YouTube, and showcases some of Chris Slane's lively privacy cartoons. People do not have to sign up for Facebook or Twitter to see what we are doing – they can view the material by clicking through from our website.

Growth in interest is slow but steady and we are developing our use of social media in a way that's relevant to our audience.

Complaints and access reviews

We received a total of 1,142 complaints in the 2011/12 year. Table 1 shows incoming and closed complaints and work in progress at year's end. Work in progress was higher than anticipated due to the extra inflow of complaints generated by the March 2012 ACC data breach.

TABLE 1: COMPLAINTS RECEIVED AND CLOSED 2007-2012

	2007/08	2008/09	2009/10	2010/11	2011/12
Complaints received	662	806	978	968	1,142
Complaints closed	767	822	961	999	1,026
Work in progress after year's end	289	273	290	247	363

The complaints process

The first aim of our complaint process is to acquire sufficient information to allow us to form a view that the complaint has substance. In cases involving refusals to provide access to information, we will review the information and

the agency's response, and make recommendations. In other cases we check for circumstances that indicate a possible breach of the Privacy Act and that exhibit some harm to the individual who is the subject of the breach. If there is substance to a complaint we try to motivate the parties to resolve the complaint.

It may be obvious early on that a complaint does not have substance in terms of the Privacy Act, for example because it is out of jurisdiction, there is no possibility of demonstrating a breach of one of the privacy principles, or there is no evidence of harm. In such cases, we will generally not notify the respondent agency – that is, we do not conduct a formal investigation. There is little point taking up the agency's time or resources in answering claims that are not going anywhere. There is also no point exposing the agency to potential litigation in the Human Rights Review Tribunal. If we do not notify a complaint, the complainant is unable to take the case to the Tribunal – the Tribunal only has jurisdiction to consider cases that we have formally investigated.

However, on occasion, there can be value in notifying an agency even if the complaint itself may not result in a view that there is an interference with privacy. Examples would be when there are multiple complaints about the same actions, or there appear to be wider systemic problems and risks that the agency will need to address to prevent harm in the future.

We can undertake own-motion investigations to look into such systemic issues, either following a complaint from an individual or on our own initiative. In these circumstances we look for obvious systemic improvements or seek assurances of a change in policy or practice.

Settlement

We aim to settle 30% of all complaints. Settlement outcomes for this year are shown in Table 2. Of the complaints closed for the year 2011/12, 30% were closed with some sort of settlement. This was an increase on our settlement rate from last year. We achieved some level of resolution in nearly 50% of the complaints that were notified.

Settlements range from apologies through to payments of money for harm caused as a result of the errant privacy practice. As in past years, monetary compensation was generally for amounts less than \$5,000, with some greater than \$10,000. Some complaints had multiple settlement outcomes such as an apology, assurances and a monetary payment.

TABLE 2: SETTLEMENT OUTCOMES 2011/12

Settlement outcome	Number
Information released	127
Apology	62
Money/monies worth	20
Information partly released	74
Information corrected	31
Assurances	22
Change of policy	22
Training	3

Personal contact

This year we achieved personal contact with one or more of the parties to a complaint on 81% (831) of the complaint files.

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

Complaints received

Past trends continue to be reflected in the incoming complaints for the year. Of the 1,142 complaints received, over 70% alleged breaches of privacy under the Privacy Act, with most of the remaining complaints alleging breaches of a Code of Practice. Table 3 shows a breakdown of these complaints.

TABLE 3: ACT/CODE – BREAKDOWN OF COMPLAINTS RECEIVED 2011/12 (PREVIOUS YEAR IN BRACKETS)

Information Privacy Principle	827	(759)
Health Information Privacy Code	288	(185)
Telecommunications Privacy Code	10	(11)
Credit Reporting Code	10	(6)
Not identified in category	7	(7)
TOTAL	1142	(968)

Agency types

Table 4 provides a breakdown of complaints in various sectors. The three major categories occupy nearly 60% of our complaints, with complaints about the public sector (51%) being the biggest overall segment.

TABLE 4: COMPLAINTS RECEIVED BY AGENCY TYPE 2011/12 (PREVIOUS YEAR IN BRACKETS)

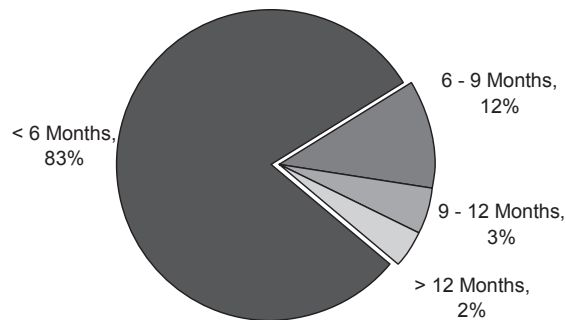
Agency Type	Total	Percentage
Government sector, including education and local authorities	441 (437)	39% (45)
Health sector, including hospitals and medical practices	133 (139)	12% (15)
Financial sector, including banking, insurance, credit agencies and debt collectors	77 (61)	7% (6)
Other	491 (331)	42% (34)
Total	1142	100%

Age of complaints

Each year, we aim to complete no less than 80% of our complaint investigations within nine months of receipt. Figure 1 demonstrates that we achieved our desired outcome by closing 95% within nine months. The remaining 5% were closed between nine and eighteen months and mostly involved protracted settlement issues.

At year's end, work in progress totalled 368 files of which 95% were under nine months old.

FIGURE 1: AGE OF CLOSED COMPLAINTS 2011/12



Top respondent agencies

This year eight agencies generated more than ten complaints each to the Privacy Commissioner. Non-government agencies have not made the top respondent list for the past four years.

Table 5 sets out the complaints received and the number closed throughout the year for top respondent agencies. In total, these agencies are responsible for 40% of the Privacy Commissioner's complaints work. The figure for ACC this year was significantly higher than usual as a result of the data breach in March.

TABLE 5: COMPLAINTS RECEIVED AND CLOSED FOR TOP RESPONDENT AGENCIES 2011/12

Agency	No of complaints received	No of complaints closed
Accident Compensation Corporation	173	62
New Zealand Police	87	91
Department of Corrections	66	57
Ministry of Social Development	60	65
Department of Labour (Immigration New Zealand)	33	37
Inland Revenue Department	12	11
Housing New Zealand	11	9
Civil Aviation Authority	10	11
TOTAL	456	347

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.

In most cases settlement totals are greater than the number of complaints with some substance. Sometimes a complaint may not have had substance, but the agency chose to act anyway. For example it may have made small changes to access decisions or given assurances to change a practice or process in the future.

Table 6 shows the various outcomes on the complaints closed for each respondent.

TABLE 6: OUTCOMES FOR TOP RESPONDENTS AGENCIES 2011/12

Agency	Closed	No interference with privacy	Complaint has some substance	Settled/mediated	Referred to Director of Human Rights Proceedings
Accident Compensation Corporation	62	46	15	16	0
New Zealand Police	91	70	21	24	2
Department of Corrections	57	43	14	20	0
Ministry of Social Development	65	51	13	16	1
Department of Labour (Immigration New Zealand)	37	21	16	20	0
Inland Revenue Department	11	10	1	1	0
Housing New Zealand	9	5	4	5	0
Civil Aviation	11	7	4	5	0

External audit

As we have done in previous years, 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 89, compared to last year's total of 91.5. The average file score was 4.5. Seventeen files scored four points or better.

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 7: REFERRALS, TRIBUNAL CASES AND OUTCOMES 2006-2012

	06/07	07/08	08/09	09/10	10/11	11/12
Referrals to Director of Human Rights Proceedings	15	20	12	18	17	5
New proceedings	22	19	29	13	25	21
Settled/withdrawn (in HRRT)	4	6	3	12	4	10
Costs awarded	5	5	4	2	6	0
Struck out	2	19	3	2	4	1
No interference	4	4	6	5	5	4
Interference	3	0	1	2	3	2

We referred five new complaints to the Director during the year. The reason for the usually low number of referrals is not obvious, except the increase in our settlement rate will have assisted. At the year's end, he was considering whether to take proceedings in 14 cases. He settled two cases, declined to take proceedings in five cases, and filed proceedings in six cases.

We decided not to refer some cases even though there was substance and the parties did not settle. This was because we believed that either nothing would be gained by further scrutiny or the formal evidence available was insufficient to support a successful case.

The Tribunal awarded compensation in both cases in which it found that an interference with privacy had occurred (*Hale v Chester Burt Funeral Home* and *Lochead-MacMillan v AML Insurance*).

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.

The most notable Commissioner-initiated inquiry during this reporting year was the inquiry into the ACC breach.

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 three applications for a section 54 exemption.

Digital switchover

The application came from the Ministry of Social Development (MSD) and the Ministry of Culture and Heritage (MCH). MCH is responsible for the move to digital television. Grants are available for people in certain categories to assist them to purchase set-top boxes. MCH required names and contact details from MSD to enable it to let these people know about the grant and to verify their eligibility.

If MSD had been responsible for administering the grant, it could have done this within the Privacy Act as it stands. Since it had to pass information to another department, however, it needed to apply for the exemption.

We were satisfied that there was a significant public benefit in identifying people who could receive the grant to help them switch to digital television and granted the exemption until February 2014. We placed conditions on the exemption, for instance that the information would only be used to contact people in relation to the grant or verify their eligibility, and that we would be informed about any complaints or data breaches relating to the information.

Veda Advantage

A law firm was attempting to locate a man who was owed money from a trust account. Veda Advantage, a major credit reporter, applied for an exemption to allow it to advise the lawyer of any up to date contact information it may have for the man. However, the law firm managed to trace the man through other means, and so Veda withdrew its application.

Ministry of Education

The Ministry of Education was sent some information by the Police about a teacher at a school. The information was unsolicited. The Ministry believed that the appropriate authority to receive the information was the school Board of Trustees. It applied for authorisation to disclose the information.

We did not grant the exemption as it was our view that an exemption was not necessary. The disclosure to the Board of Trustees was permitted under the Privacy Act since the Board of Trustees was clearly the appropriate authority to receive it rather than the Ministry. We advised the Ministry that if it did not wish to make the disclosure itself, it could suggest that the Police make the disclosure directly to the Board of Trustees.

Policy

The Office's policy function supports improved privacy practices in government and business by providing advice to:

- Cabinet and Parliament on the privacy implications of legislative proposals and other privacy initiatives
- the private and public sectors on new technology issues, including by producing guidance
- the health sector on protecting personal information.

Legislation and other government policy

Our advice on legislation and public sector policy 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.

This function ensures that government and parliament take into account potential costs to New Zealanders' privacy when they create new laws.

We assess the impact of our advice on whether we are able to achieve substantive changes to legislation before it is passed.

The Office provided advice on 57 agency files:

- 68% of these files raised privacy issues that we considered needed further consideration
- 87% of files requiring further consideration saw some improvement as a result of our advice
- 15% were “substantively” improved as a result of our advice.

Our goal for future years is to reduce the percentage of files requiring action by encouraging agencies to undertake deeper privacy analysis before approaching the Office. We also aim to increase the proportion of files improved, in particular those that are substantively improved as a result of the advice we provide.

Major legislative projects the Office contributed to in 2011/12 include:

- Electronic Identity Verification Bill
- Social Security (Youth Support and Work Focus) Amendment Act 2012
- Privacy (Information Sharing) Bill
- Victims of Crime Reform Bill
- Land Transport Management Amendment Bill.

At the policy level, our most significant individual file has been the Privacy Act reforms, involving discussions with the Ministry of Justice and others. We have also made contributions to policy development in important areas such as border control, identity management, and protection of vulnerable children.

Health advice

Health information privacy raises specific issues of its own, particularly in the context of a national and international push towards the development of electronic health records, and the expansion of regional clinical data repositories and shared care initiatives. In recognition of this, the Office has a memorandum of understanding with the Ministry of Health which funds advice on health privacy issues. The Office’s independence from the Ministry is fully preserved.

Major projects during 2011/12 included the Office continuing to advise the National Health IT Board on electronic health records, and working on proposed amendments to the Health Information Privacy Code. The Office has also maintained an active programme of awareness-raising through speaking engagements and articles on privacy issues targeted at the health sector.

Technology advice

The Office’s efforts to improve privacy practice in the private sector tend to be focused on supporting New Zealand business to better understand privacy risks and solutions in order to realise the benefits of new technology. The Office keeps a close watch on new and developing technologies so that it is well placed to deliver comprehensive and timely advice.

Cloud computing has been the focus of the Office's efforts during 2011/12. We have supported industry efforts to develop a code of conduct for cloud computing providers, including providing expert advice on privacy issues. We have also substantially completed work on privacy guidelines for small and medium enterprises that are considering using cloud computing services. The guidance will be released later in 2012.

Information matching

Under the Privacy Act, 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 Act, and we monitor and report their compliance with those requirements.

Details of our information matching activities this year, and reports on the 50 active government sector 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 further proposed code was released for public comment, the National Emergency Civil Defence (Information Sharing) Code.

Credit Reporting Privacy Code

As a result of a thorough review, the Privacy Commissioner decided to amend the Code to enable New Zealand to move to more comprehensive credit reporting. Reviews of privacy and credit law in Australia led the Australian Government to move in a similar direction. We 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 amended the code in two stages. The first stage, Amendment No.4, completed a public submission process during 2010 and was issued in December 2010. Amendment No.5 was publicly notified as a proposal in May 2011. Public hearings of submissions were held in July and Amendment No. 5 was issued in September 2011 and came into force, together with Amendment No.4 in April 2012.

The amendments represent a fundamental shift in credit reporting in New Zealand. The new system will, for the first time, allow credit reporters to collect records on the actual amounts of credit extended to individuals. Lenders will

upload information, on a monthly basis, showing whether or not individuals have met their monthly credit repayments.

The new system will amass much larger collections of detailed and sensitive financial information on New Zealanders. The Code changes have introduced special measures to ensure a high level of compliance and to provide protections to individuals. A new system of 'credit freezes' was introduced for individuals who are at special risk of identity fraud.

The pay-off for New Zealand and individuals should be a much enhanced ability to assess creditworthiness. There is international evidence to suggest that this can bring economic benefits in terms of risk management for business and improved credit arrangements for individuals.

Proposed Civil Defence National Emergencies (Information Sharing) Code

Last year the Privacy Commissioner issued the Christchurch Earthquake (Information Sharing) Code within 48 hours of the major Christchurch earthquake on 22 February, 2011. 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, had sufficient authority to share personal information as needed. The code was a temporary expedient and expired after four months.

Prior to its expiry, the Office reviewed the code's usefulness with stakeholders. We concluded that it had been worthwhile. We later decided that it would be useful to have a similar code in place in case New Zealand was ever again faced by a national emergency.

Accordingly, we publicly notified a proposed code in April and sought public submissions. The submission process closed in late May and at the end of the year, the submissions received were still being considered.

The proposed code, like the temporary Christchurch code, would supplement the existing law and provide additional authority to collect and disclose personal information. In particular, it would provide 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 a national emergency. In particular, the code would provide that 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 services, 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.

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 22 (last year, 52) consultations from the Ombudsman and completed and closed 20. All consultations were completed within two months of receipt.

Like previous years, the privacy interests that gave rise to the most consultations were those dealing with employment issues within the government. Several related to access to information about criminal investigations.

3: REPORT ON ACTIVITIES

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 and international issues.

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 and accounting work for the Office.

Equal employment opportunities

The Office of the Privacy Commissioner promotes Equal Employment Opportunities (EEO) to ensure that its practices are in line with its obligations as a good employer. The Office of the Privacy Commission has an EEO policy that is integrated with the human resource programmes outlined in the Statement of Intent 2011 and that encourages active staff participation in all EEO matters. These are reviewed annually.

During the 2011/12 year, the main areas of focus have been:

- developing talent within the Office regardless of gender, ethnicity, age or other demographic factor
- the Privacy Commissioner continuing in her role as a board member of the Equal Opportunities Trust
- the integration of new work practices that promote or enhance work life balance amongst employees
- maintaining equitable gender-neutral remuneration policies, which are tested against best industry practice.

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

TABLE 8: WORKPLACE GENDER PROFILE 2011/12

	Women		Men		Total
	Full-time	Part-time	Full-time	Part-time	
Commissioner	1				1
Senior managers	1		3		4
Team leaders/Senior Advisers	3	1	4		8
Investigating officers	5				5
Administrative support	5	2			7
Advisers (Technology & Policy)	1	1	2		4
Enquiries officers	1		1		2
Total	17	4	10		31

TABLE 9: WORKPLACE ETHNIC PROFILE 2011/12

	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/ Senior advisers									7	1
Investigating officers					1				3	1
Administrative support									5	2
Advisers (Technology & Policy)									3	1
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 to find 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 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
- 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 to find some wrongdoing.

The Privacy Act regulates 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 (rule 1)
- limiting the disclosure and use of information (rule 4)
- 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 is on the 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 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 Credit (formerly Family Support Tax Credits)

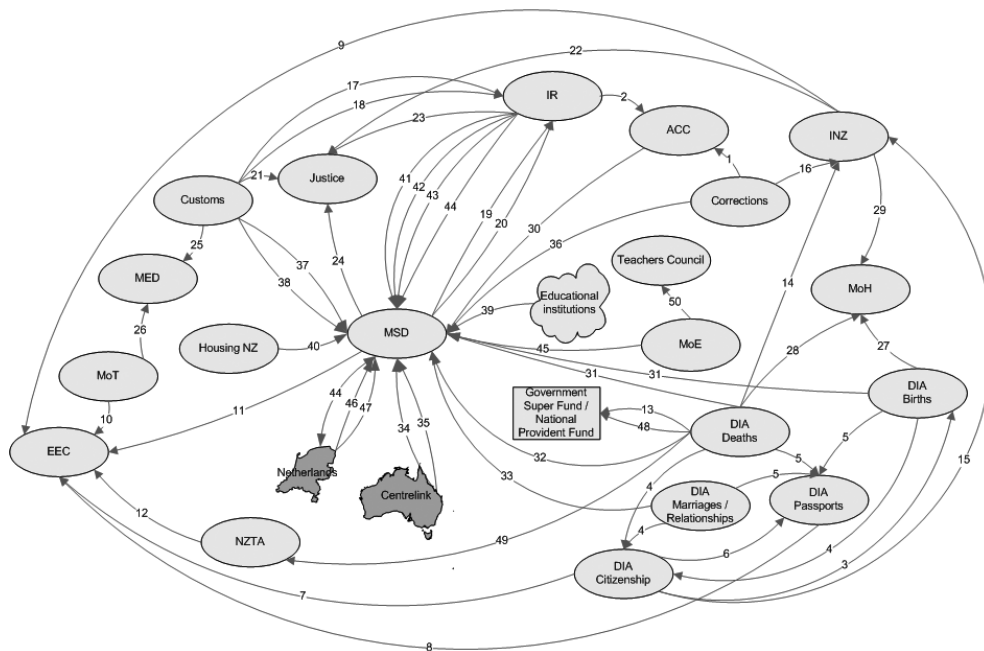
The year in information matching

Our oversight of information matching during the year included:

- monitoring 50 active programmes
- reporting to the Minister of Justice on a periodic review (s.106) of four information matching programmes.

Figure 4 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 2: ACTIVE AUTHORISED INFORMATION MATCHING PROGRAMMES 2011/12



Outreach

In April we updated our web page for information matching reports and reviews to provide online copies of all the information matching reports. The page is available at <http://privacy.org.nz/information-matching-reports-and-reviews/>

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

The Office ran one information matching workshop in March 2012 for eight staff from Inland Revenue.

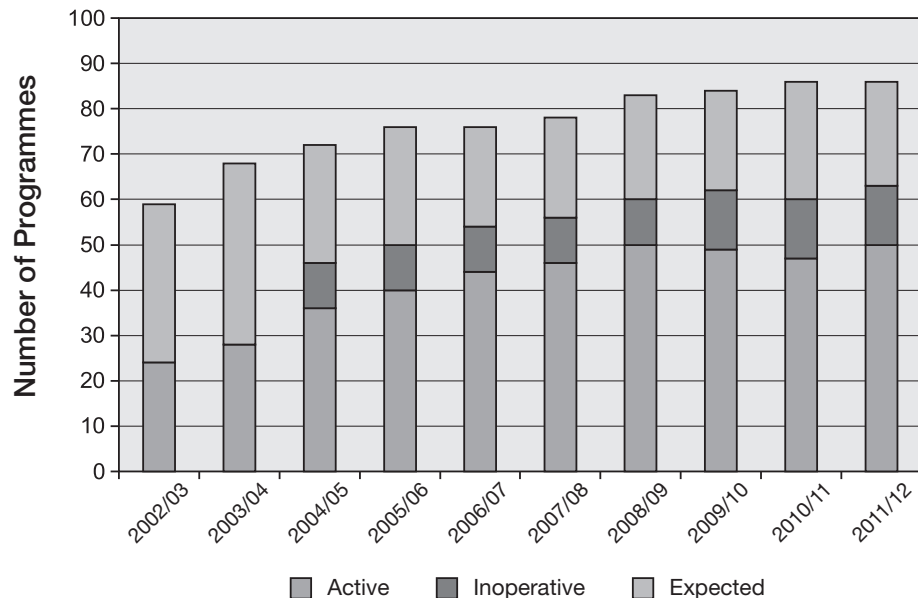
Changes in authorised and operating programmes

Parliament passed one new information matching authorisation during the year. The Electoral (Administration) Amendment Bill (No 2) was passed on 16 August 2011, authorising the now active DIA(Passports)/EEC Unenrolled Voters Programme.

The Ministry of Health has started using Immigration New Zealand information to check claims for funding by Public Health Organisations.

The BDM(Births)/MoE Student Birth Confirmation Programme restarted in May 2012. Results of matching activity will be reported next year.

FIGURE 3: AUTHORISED, OPERATING AND INOPERATIVE INFORMATION MATCHING PROGRAMMES 2003-2012



Periodic review (s.106) of information matching programmes

In August 2011 we reported to the Minister of Justice on a periodic review (s.106) of four information matching programmes (NZTA/EEC Unenrolled Voters; MOT/EEC Unenrolled Voters; MSD/EEC Unenrolled Voters; Citizenship/EEC Unenrolled Voters). We recommended that these programmes continue. 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 2012, 33 of the 50 active programmes used online transfers.

TABLE 10: FIRST TIME ONLINE TRANSFER APPROVALS 2011/12

User agency Programme name (and number) Approval date	Reasons for granting	Grounds in support
ACC		
Compensation and Levies (programme 2) 25 January 2012	efficiency and security	acceptable controls
Ministry of Justice		
Fines Defaulter Tracing (programme 24) 18 July 2011	efficiency and security	acceptable controls
Ministry of Health		
Publicly Funded Health Eligibility (programme 29) 25 November 2011	efficiency and security	acceptable controls

TABLE 11: RENEWED APPROVALS 2011/12

User agency Programme name (and number) Approval date	Reasons for granting	Grounds in support
Department of Internal Affairs		
Passport eligibility (programme 5) 25 November 2011	continued efficiency	satisfactory audit result
Passport eligibility (programme 6) 25 November 2011	continued efficiency	satisfactory audit result
Citizenship application processing (programme 4) 28 November 2011	efficiency & security	timely delivery of data
Passport eligibility (programme 5) 18 April 2012	continued efficiency	satisfactory audit result
Immigration New Zealand		
Prisoners (programme 16) 5 June 2012	continued efficiency	satisfactory operation and enhanced security measures
Ministry of Social Development		
Change in circumstances (programme 34) 23 December 2011	efficiency & security	timely delivery of data
Netherlands general adjustment (programme 47) 22 June 2012	efficiency & security	satisfactory audit result

Prisoners (programme 36) 27 June 2012	efficiency & security	satisfactory operation and enhanced security measures
Deaths (programme 32) 27 June 2012	efficiency & security	satisfactory operation and enhanced security measures
Marriages (programme 33) 27 June 2012	efficiency & security	satisfactory operation and enhanced security measures

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.

2011/12 activity:

Match runs	50
Records received for matching	87,423
Possible matches identified	3,304
Overpayments established (number)	44

Overpayments established	\$26,323
Average overpayment	\$598
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 online transfer.

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.

2011/12 activity:

Self-employed people's records received for matching	530,665
Employers' records received for matching	573,778
Invoices issued to self-employed people	348,349
Invoices (individual employee) issued to employers	448,764
Challenges by individuals	48
Challenges by corporations	49
Total challenges	97
Successful challenges	3

Compliance: Compliant.

3 Citizenship/BDM Citizenship by Birth Processing Programme

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

Year commenced: 2006

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

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

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

2011/12 activity:

Births registered	62,255
Notices of adverse action	1,425
Challenges received	347
Successful challenges	202
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.

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.

2011/12 activity:

Applications for citizenship by descent (may include more than one person)	10,004
Notice of adverse action (arising from failure to match)	7
Successful challenges	6
Citizenship by descent registered	9,331

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.

2011/12 activity:

Passport applications	608,007
Possible matches: Births	1,343,713
Possible matches: Marriage/Relationships	102,893
Possible matches: Deaths	2,487,321
Notice of adverse action	6,523
Successful challenges	6,481
Passports issued (diplomatic, official and standard)	603,765

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

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

The difference between the number of applications and the number of passports issued primarily reflects applications that are being processed when statistics were compiled.

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.

2011/12 activity:

Passport applications	608,007
Possible matches to Citizenship records	573,136
Notice of adverse action	744
Successful challenges	738
Passports issued (diplomatic, official and standard)	603,765

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.

The difference between the number of applications and the number of passports issued primarily reflects the number of applications being processed when statistics were compiled.

Compliance: Compliant.

7 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).

2011/12 activity:

Match runs	4
Records received for matching	71,971
Invitations to enrol sent out	788
Presumed delivered	774
New enrolments	104
Percentage of letters delivered resulting in changes	15%
No response	670
Cost	\$920
Average cost per enrolment	\$8.85

Commentary: The figure for 'Records received for matching' is significantly higher than the figure reported in 2010/11 (10,600), because it includes any name changes and alternate names.

Compliance: Compliant.

8 DIA (Passports)/EEC Unenrolled Voters Programme

Purpose: To compare passport records 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: 2011

Features: Data transferred on request by CD.

DIA (Passports) disclosure to EEC: Passports provides full name, date of birth and residential address of passport holders aged 17 years and over

2011/12 activity:

Match runs	2
Records received for matching	413,196
Invitations to enrol sent out	23,207
Presumed delivered	22,131
New and updated enrolments	4,513
Percentage of letters delivered resulting in changes	20%
No response	17,618
Cost	\$17,227
Average cost per enrolment	\$3.82

Compliance: Compliant.

9 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 identified because five separate files are received, each relating to a different permit type.

2011/12 activity:

Records received for matching (on 30 June 2012)	207,766
Possible matches identified	1,502
Notice of adverse action sent ⁶	1,202
Challenges received	54
Successful challenges	45
Removals from roll or not added to roll	1,457
Cost	\$13,856
Average cost per removal	\$9.51

Commentary: In August 2011 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). From September 2011 EEC has contacted people by phone where possible to discuss their eligibility. Letters are still sent to confirm the conclusion reached during the phone call.

Compliance: Compliant.

10 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.

2011/12 activity:

Match runs	4
Records received for matching	1,316,722
Invitations to enrol sent out	142,410
Presumed delivered	135,712
New and updated enrolments	25,736
Percentage of letters delivered resulting in changes	19%
No response	109,976
Cost	\$103,934
Average cost per enrolment	\$4.04

Compliance: Compliant.

⁶ Not counting follow up letters to phone conversations where the applicant is advised they are not eligible.

11 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.

2011/12 activity:

Match runs	4
Records received for matching	659,980
Invitations to enrol sent out	110,081
Presumed delivered	106,944
New and updated enrolments	18,651
Percentage of letters delivered resulting in changes	17%
No response	88,293
Cost	\$80,162
Average cost per enrolment	\$4.30

Compliance: Compliant.

12 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.

2011/12 activity:

Match runs	4
Records received for matching	935,560
Invitations to enrol sent out	146,970
Invitations presumed delivered	141,015
New and updated enrolments	26,466
Percentage of letters delivered resulting in changes	19%
No response	114,549
Cost	\$106,128
Average cost per enrolment	\$4.01

Compliance: Compliant.

13 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).

2011/12 activity:

Records received for matching	30,501
Possible matches identified	9,333
Notices of adverse action sent	679
Challenges	0

Compliance: Compliant.

14 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 information 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.

2011/12 activity:

Match runs	2
Records received for matching	30,358
Possible matches identified	897
Records marked as deceased - overstayer list	121
Records marked as deceased - temporary visa holders' list	56
Total number of records updated as deceased	177

Compliance: Compliant.

15 Citizenship/INZ Entitlement to Reside Programme

Purpose: To 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.

2011/12 activity:

Match runs	3
Records received for matching	1,199,788
Possible matches identified	6,919
Number of NZ citizens removed from the overstayer list	427

Commentary: INZ has performed two match runs to cover the current period, and one match using historical records previously received. Historical records are used to identify individuals who have been added to INZ's temporary visa-holder records because they have returned to New Zealand using their non-New Zealand passport.

The number of possible matches doubled from 2010-11(2848) after INZ started using new data matching software. The number of NZ citizens removed from the overstayer list increased by 15 per cent (373 in 2010-11).

Compliance: Compliant.

16 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 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.

2011/12 Activity:

Match runs	53
Possible matches identified	364
Cases excluded as not being eligible for removal or deportation	329
Notices of adverse action	35
Successful challenges	1
Cases considered for removal and deportation	33
Removals and deportations from NZ at year's end	30

Commentary: On 1 December 2011, the Corrections (Immigration Information Disclosure) Regulations 2011 came into force. The regulations enable INZ and Corrections to extend the scope of the programme to include home detention and community-based sentencing records. During June 2012, INZ tested the inclusion of home detention records. Currently, INZ only receives records for individuals serving prison sentences.

An audit, required as a condition on the use of online transfers, found that encryption standards may not have been met. To remedy this issue, additional file encryption was implemented and became a requirement for future transfers from June 2012.

Compliance: Compliant but see comments.

17 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: 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).

2011/12 Activity:

Possible matches identified	7,108
Arrival cards received for liable parents	1,034
Cards not useable or did not meet matching criteria	108
Remaining cards where contact attempted with liable parent	926
New contact details updated	413
Existing contact details confirmed	228
Contact details not useful	285

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

Compliance: Compliant.

18 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.

2011/12 Activity: There were 485,464 borrower records (441,206 last year) updated as a result of matching student borrower records with travel movement information held by Customs.

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

Compliance: Compliant.

19 MSD/IR Working For Families Tax Credits Administration Programme

Purpose: To inform IR of beneficiaries who have ceased or commenced paid employment so that IR can stop or start paying 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.

2011/12 Activity: 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.

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

Compliance: Compliant.

20 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.

2011/12 Activity: Inland Revenue estimate annual savings of \$4.2 million from operating this programme. This represents the maximum potential savings possible if double payments identified continued to be paid until the end of the year.

The actual number and value of payments stopped during the year was 1,089 and \$309,488 respectively.

Commentary: An audit on the operation of this programme found that there are effective controls in place but it noted that work to refresh the information matching agreement has been delayed. That work commenced in December 2008 but has yet to be completed. Inland Revenue management have committed to liaise with MSD to complete the project.

Compliance: Compliant but see comment.

21 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:

- have outstanding fines of \$1000 or more and
- a warrant to arrest (which covers part of the outstanding fines) has been issued.

Silent alert results are transferred to Justice for use in the INZ/Justice Fines Defaulters Tracing Programme (programme 22)

Interception alerts are created for fines defaulters where:

- any amount of reparation is owing and a warrant to arrest (which covers part of the reparation outstanding) has been issued or
- court-imposed fines of \$5000 or more are outstanding and a warrant to arrest (which covers part of the court-imposed fines outstanding) has been issued.
- Interception alerts result in travellers being intercepted as they cross the border.

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.

2011/12 Activity:

Silent alerts triggered	5,111
Individuals subject to silent alerts	2,394
Intercept alerts triggered	175
People intercepted ⁷	149
On departure	50
On arrival	119
Incorrect intercepts	23
Fines had already been paid	6
Wrong person identified by the match	17
Interception not completed	16
Fines received	\$110,546
Reparation received	\$155,061
Amount under a current time to pay arrangement	\$121,680
Remittals/ Alternative sentence imposed	\$85,703

Commentary: There have been modest increases in payments received for fines, reparations, and amounts under a current time-to-pay arrangement.

As at 30 June, there were 3,701 fines defaulters who had interception alerts recorded against their names in Customs records, up from 2,888 last year. There were also 21,267 fines defaulters who had silent alerts recorded, up from 16,596 last year.

In October 2011, Justice implemented new workflow software to help staff manage fines defaulter records. Justice believes the new software is likely to be the reason behind an increase in warrants to arrest being issued, and consequently a 28% increase in fines defaulters recorded on both silent and intercept alert databases.

Compliance: Compliant.

22 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.

⁷ A person may trigger more than one intercept alert in a given period.

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).

2011/12 Activity:

Records sent to INZ	4,724
Notices of adverse action	886
Successful challenges	3
Payment received for fines	\$180,848
Amounts under a current time-to-pay arrangement	\$91,920
Remittals/alternative sentence imposed	\$195,223

Commentary: In October 2011, Justice changed its process of how it uses information obtained from this programme. Formerly a dedicated group in Justice was responsible for processing the data. Justice's new approach involves match results being added to a national work queue that is processed by staff throughout New Zealand. This has led to delays in actioning the match results and recovering fines.

Compliance: Compliant.

23 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. From 15 October, transfers occur daily using encrypted USB stick.

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.

From 15 October, the unique identifier transferred is the 'Data Matching Reference Number' which is generated and used only for the purposes of this programme.

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

From 15 October, IR returns the current address and all known telephone numbers for the person, the name, address, and contact numbers of the person's employer or employers, and the unique identifier originally provided by Justice.

2011/12 Activity:**Processing Activity**

	July to December 2011	January to June 2012
	Final figures	Progress figures
Match runs	46	117
Records sent for matching	310,848	1,051,819
Possible matches identified	151,005	389,435
Notices of adverse action	111,557	134,660
Challenges	519	954
Successful challenges	158	220

Financial Outcome Activity

		July to December 2011	January to June 2012
		Final figures	Progress figures
Paid/settled (\$)	IR	12,881,077	10,169,974
	MSD	8,873,025	8,052,498
	Both	4,565,264	7,580,210
Total paid/settled (\$)		26,319,366	25,802,682
People with payment or remittal	IR	22,227	26,235
	MSD	11,866	18,331
	Both	7,994	20,534
Total people with payment or remittal		42,087	65,100

Commentary: A new daily matching process started on 15 October 2011. Under the new process, there has been a large increase in matching activity.

This programme operates in conjunction with the MSD/Justice Fines Defaulters Tracing programme (24). We report combined totals for both programmes because Justice cannot always determine which programme resulted in the payment of outstanding fines. In those cases Justice has reported amounts paid/settled under the heading of 'both'.

A new reporting regime is in place this year. We report 'progress figures' for matches where the amounts paid/settled are still being calculated (less than six months since a notice of adverse action sent) and 'final figures' for matches where the calculation of amounts paid/settled has been completed. 'Final figures' updating the 'progress figures' published here will be provided on our website at the end of the next six monthly reporting period.

Compliance: Compliant.

24 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. From 15 October 2011, data transferred daily by online transfer.

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.

From 15 October 2011, the unique identifier transferred is the 'Data Matching Reference Number' which is generated and used only for the purposes of this programme.

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

From 15 October 2011, MSD returns the last known residential address, postal address, residential, cell-phone and work phone numbers, and the unique identifier originally provided by Justice.

2011/12 Activity:

Processing Activity

	July to December 2011	January to June 2012
	Final figures	Progress figures
Match runs	34	115
Records sent for matching	252,653	1,007,866
Possible matches identified	82,330	243,187
Notices of adverse action	69,004	92,030
Challenges	265	529
Successful challenges	91	139

Financial Outcome Activity

		July to December 2011	January to June 2012
		Final figures	Progress figures
Paid/settled (\$)	IR	12,881,077	10,169,974
	MSD	8,873,025	8,052,498
	Both	4,565,264	7,580,210
Total paid/settled (\$)		26,319,366	25,802,682

People with payment or remittal	IR	22,227	26,235
	MSD	11,866	18,331
	Both	7,994	20,534
Total people with payment or remittal		42,087	65,100

Commentary: A new daily matching process started on 15 October 2011. Under the new process, there has been a large increase in matching activity.

This programme operates in conjunction with the IR/Justice Fines Defaulters Tracing programme (23). We report combined totals for both programmes because Justice cannot always determine which programme resulted in the payment of outstanding fines. In those cases Justice has reported amounts paid/settled under the heading of 'both'.

A new reporting regime is in place this year. We report 'progress figures' for matches where the amounts paid/settled are still being calculated (less than six months since a notice of adverse action sent) and 'final figures' for matches where the calculation of amounts paid/settled has been completed. 'Final figures' updating the 'progress figures' published here will be provided on our website at the end of the next six monthly reporting period.

Compliance: Compliant.

25 Customs/MED Motor Vehicle Traders Importers Programme

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

Year commenced: 2004

Features: Data transferred monthly by online transfer.

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

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

2011/12 Activity:

Match runs	4
Records received for matching	1,371
Individuals or entities of interest identified	15
Notices of adverse action sent	17

Successful challenges	Entities: registered under another name	0
	Entities: primary purpose not financial gain	3
Entities referred to the National Enforcement Unit		0
Registrations as a result of notices of adverse action		4
No response to letters		8

Commentary: MED restarted this programme in March 2012. The programme was placed on hold about two years ago due to limited staff resources. Since restarting the programme, MED has refined its business decision processes, resulting in a reduced number of notices of adverse action.

Many of the letters result in no response. For these cases, MED monitors to see if importing activity continues, and may take further action.

Compliance: Compliant.

26 MOT/MED Motor Vehicle Traders Sellers Programme

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

Year commenced: 2003

Features: Data transferred monthly by online transfer.

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

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

2011/12 Activity:

Match runs		2
Records received for matching		4,808
Individuals or entities of interest identified		139
Notices of adverse action sent		139
Successful challenges	Entities: registered under another name	4
	Entities: primary purpose not financial gain	31
Entities referred to the National Enforcement Unit		0
Registrations as a result of notices of adverse action		22
No response to letters		82

Commentary: MED restarted this programme in May 2012. It was placed on hold about two years ago due to limited staff resources. Since restarting the

programme, MED has refined its business decision processes, resulting in a reduced number of notices of adverse action.

Many of the letters result in no response. For these cases, MED monitors to see if selling activity continues, and may take further action.

Compliance: Compliant.

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

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

Year commenced: 2009

Features: Data transferred monthly 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.

2011/12 activity:

Records received for matching	62,022
Possible matches identified	62,022
Records not matched	0

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

Compliance: Compliant.

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

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

Year commenced: 2009

Features: Data transferred monthly on CD.

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

2011/12 activity:

Records received for matching	29,981
Possible matches identified	26,368
Records manually matched	3,502
New NHIs allocated	111
Corrections to matches (including from previous years matches)	22

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.

29 INZ/MoH Publicly Funded Health Eligibility Programme

Purpose: To enable MoH to determine an individual's:

- Eligibility for access to publicly funded health and disability support services; or
- Liability to pay for publicly funded health and disability support services received.

Year commenced: 2011

Features: Data transferred on request by online transfer.

MoH disclosure to INZ: MoH sends names, date of birth and NHI number to INZ for matching.

INZ disclosure to MoH: INZ provides names, gender, birth date, nationality, visa or permit type and start and expiry dates, and dates the person entered or left New Zealand. INZ may also disclose details of a parent or guardian of a young person.

2011/12 activity:

Records sent for matching		76,000
Records matched		52,530
Notices of adverse action		1,903
Successful challenges	(wrongly matched)	2
	(error in application of eligibility criteria)	61

Commentary: The 61 'successful challenges' include 40 dual citizens who were listed as 'visitors' in Immigration's records as they had used a foreign passport on their return to New Zealand.

Compliance: Compliant.

30 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 is transferred weekly by online transfer.

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

- 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 or
- current claims that have continued for one year since the first payment.

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

2011/12 Activity:

MSD's eligibility checking ensures current clients are being paid their correct entitlements.

Eligibility checking results

New match runs started in the reporting period	
Match runs	52
Records received for matching	1,727,767
Possible matches identified	5,333
All processing activity during the reporting period	
Matches that required no further action	3,371
Notices of adverse action	2,033
Challenges	48
Successful challenges	33
Overpayments established	1,382
Value of overpayments established	\$1,473,889

MSD receives debt recovery notifications for all former (non-current) clients who have outstanding benefit debt. The notifications enable MSD to re-establish contact with debtors, or to maintain accurate contact information.

Debt recovery notification results

Notifications received	5,675
Notices of adverse action	156
Challenges	0
Debtors under arrangement to pay	44
Balance owed under arrangement	\$182,855
Debtors paid in full	10
Total recovered	\$16,471

Commentary: This is the first year of detailed reporting about MSD's use of ACC data to recover debts from former clients. In the coming year MSD intends to tighten the matching algorithm settings for debt recovery notifications to reduce the number of false positive matches.

Compliance: Compliant.

31 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.

2011/12 Activity:

Benefit applications processed	351,897
Possible matches identified	21,154
All processing activity in the reporting period	
Matches that required no further action	1,650
Cleared cases	19,805
Cases referred for further investigation	369
Letters advising update of information	313
Notices of possible adverse action	50
Challenges	0
Overpayments established	0
Value of overpayments established	0

Commentary: The 'cleared cases' figure represents the number of MSD client records updated as a result of minor differences between the information input into MSD's systems and the information received from BDM. MSD only sends a letter to the client if it adds information onto the client record that was not originally provided by the client.

Compliance: Compliant.

32 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.

2011/12 Activity:

New match runs started in the reporting period	
Match runs	52
Records received for matching	30,049
Possible matches identified	5,031
All processing activity in the reporting period	
Matches that required no further action	2,464
Notices of adverse action	2,520
Challenges	0
Overpayments established	348
Value of overpayments established	\$423,183

Commentary: An audit, required as a condition on the use of online transfers, found that encryption on DIA's secure 'drop-box' did not meet the required standard. The issue was resolved after DIA upgraded the level of encryption to an acceptable level.

Compliance: Compliant but see comments.

33 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 is 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.

2011/12 Activity:

New match runs started in the reporting period	
Match runs	52
Records received for matching	22,527
Possible matches identified	2,887
All processing activity in the reporting period	
Matches that required no further action	1,728
Notices of adverse action	1,169
Challenges	1
Successful challenges	1
Overpayments established	486
Value of overpayments established	\$730,087

Commentary: An audit, required as a condition on the use of online transfers, found that encryption on DIA's secure 'drop-box' did not meet the required standard. The issue was resolved after DIA upgraded the level of encryption to an acceptable level.

Compliance: Compliant but see comments.

34 Centrelink/MSD Change in Circumstances Programme

Purpose: For MSD and Centrelink (the Australian Government agency administering social welfare payments) to exchange benefit and pension applications, and changes of client information.

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.

2011/12 activity:

Changes of information received by MSD from Centrelink	619,347
Notices of adverse action	7,617
Changes of information sent by MSD to Centrelink	242,494

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

of Residence Programme [see programme 35 on this page].

Compliance: Compliant.

35 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.

2011/12 activity:

Records received back from Centrelink	6,953
Australian pensions granted	0

Notices of adverse action are recorded under the Centrelink/MSD Change in Circumstances Programme [see programme 34 on previous page].

Commentary: This programme was stopped by Centrelink in January 2012 over concerns that Centrelink was accessing information about people who were not Centrelink clients. MSD is talking with Centrelink to restore the programme.

An audit of the online transfer identified that the sample file was not being deleted when transferred as the person had not been granted deletion rights. This has been resolved.

This is the third year in which no one from the sample has gained an Australian pension as a direct result of the match. MSD prefers to continue with the match as operating costs are low and the savings that result when Australia pays part of superannuation entitlements are cumulative over the years.

Compliance: Compliant.

36 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, Corrections sends MSD details about all prisoners who are received, on muster or released from prison. 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.

2011/12 Activity:

MSD's eligibility checking ensures current clients are being paid their correct entitlements.

Eligibility checking results

New match runs started in the reporting period	
Match runs	359
Records received for matching	17,201,022
Possible matches identified	13,687
All processing activity in the reporting period	
Matches that required no further action	4,904
Notices of adverse action	8,768
Challenges	9
Successful challenges	5
Overpayments established	2,754
Value of overpayments established	\$380,960

MSD receives debt recovery notifications for all former clients who have outstanding debt. The notifications enable MSD to re-establish contact with debtors, or to maintain accurate contact information.

Debt recovery notification results

Notifications received	17,364
Notices of adverse action	341
Challenges	0
Debtors under arrangement to pay	13
Balance owed under arrangement	\$114,026.91
Debtors paid in full	11
Total recovered	\$3,310.01

Commentary: This is the first year of detailed reporting about MSD's use of Corrections data to recover debts from former clients. In the coming year MSD intends to tighten the matching algorithm settings for debt recovery notifications to reduce the number of false positive matches.

An audit, required as a condition on the use of online transfers, found that encryption standards may not have been met. To remedy this issue, additional file encryption was implemented and became a requirement for future transfers from July 2012.

Compliance: Compliant but see comments.

37 Customs/MSD Arrivals & 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 is transferred weekly by online transfer.

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

2011/12 Activity:

MSD's eligibility checking ensures current clients are being paid their correct entitlements.

Eligibility checking results

New match runs started in the reporting period	
Match runs	53
Records received for matching	10,071,923
Possible matches identified	52,775
All processing activity in the reporting period	
Matches that required no further action	22,367
Notices of adverse action	30,459
Challenges	165
Successful challenges	147
Overpayments established	18,511
Value of overpayments established	\$13,068,536

MSD receives debt recovery notifications for all former clients who have outstanding benefit debt. The notifications enable MSD to re-establish contact with former clients and to maintain accurate contact information.

Debt recovery notification results

Notifications received	84,696
Notices of adverse action	1,880

Challenges	0
Debtors under arrangement to pay	197
Balance owed under arrangement	\$563,570.02
Debtors paid in full	135
Total recovered	\$98,015.25

Debt recovery baseline – one off match results (see commentary)

Debtors matched	26,476
Debtors identified as returned to NZ	2,185
Notices of adverse action	660
Challenges	0
Debtors under arrangement to pay	39
Balance owed under arrangement	\$42,413.99
Debtors paid in full	19
Total recovered	\$22,716.74

Commentary: This is the first year of detailed reporting on MSD's use of Customs data to recover debts from former clients. In the coming year MSD intends to tighten the matching algorithm settings for debt recovery notifications to reduce the number of false positive matches. MSD also intends to make changes so that notifications for debtors owing smaller amounts will not be created until it is confirmed that they have been overseas for a more significant period.

A one-off match using Customs arrival and departure information was completed in November 2011 to identify debtors who had left or returned to New Zealand between 1996 and 2011. The match enabled MSD to follow up on debtors who had returned to New Zealand, and to confirm its overseas debtors prior to commencing the use of Customs data match notifications.

Compliance: Compliant.

38 Customs/MSD Periods of Residence Programme

Purpose: To enable MSD to confirm periods of residence in New Zealand or overseas to determine eligibility for any benefit.

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.

2011/12 activity: MSD staff accessed 194 Customs records.

Commentary: An audit on the operation of this programme found that there are effective controls in place but some records may not have been disposed of

within one month as required by the agreement with Customs. MSD has changed to a fortnightly cycle to avoid this.

Compliance: Compliant.

39 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 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.

2011/12 activity:

Educational institutions involved in the matching programme	625
Records sent for matching	976,350
Individual applicants involved in matching	227,715
Notices of adverse action sent out (individuals may receive more than one)	42,660
Percentage of applicants issued a notice of adverse action	19%
Challenges	135
Successful challenges	75
Decisions to decline loan/allowance	24,315

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

Compliance: Compliant.

40 HNZ/MSD Benefit Eligibility Programme

Purpose: To enable MSD to detect:

People incorrectly receiving accommodation assistance while living at subsidised HNZ properties

- 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 boarders), relationship details (to other tenants) and details of any dependants. Also included are details about the property location, tenancy start and end dates, weekly rental charges and any forwarding address provided on termination of the tenancy.

2011/12 Activity:

New match runs started in the reporting period	
Match runs	52
Records received for matching	86,157
Possible matches identified	6,024
All processing activity in the reporting period	
Matches that required no further action	6,095
Notices of adverse action	53
Challenges	0
Overpayments established	28
Value of overpayments established	\$49,474

Compliance: Compliant.

41 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, or
- were included by random selection.

Each record provided to IR includes the surname, first initial, date of birth, IRD number, 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, IRD number, employer's name, address, email and phone contact details, and employment commencement and cessation dates.

2011/12 Activity:

New match runs started in the reporting period	
Match runs	12
Records sent for matching	147,795
Possible matches identified	24,012
All processing activity in the reporting period	
Matches that required no further action	13,647
Notices of adverse action	8,681
Challenges	121
Successful challenges	25
Overpayments established	4,280
Value of overpayments established	\$31,012,155

Commentary: The value of overpayments established in 2011/12 is the largest since this programme commenced in 1993. MSD attributes the results to the changes made in November 2010 which enabled it to make more informed decisions about which records to check.

From May 2012, MSD has limited the records sent for matching through this programme to those involving cases of suspected fraud. The change in practice is in anticipation of the programme being replaced by a new information sharing system. The new system, authorised by section 81BA of the Tax Administration Act 1994, is expected to go live in the final quarter of the 2012 calendar year.

Compliance: Compliant.

42 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 monthly 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,

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, MSD client number, employer's name, address, email and phone contact details, and employment commencement and cessation dates.

2011/12 Activity:

New match runs started in the reporting period	
Match runs	9
Records sent for matching	50,162
Possible matches identified	24,067
All match runs active in the reporting period	
Matches that required no further action	9,189
Notices of adverse action	16,167
Challenges	217
Successful challenges	134
Overpayments established	4,862
Value of overpayments established	\$6,627,498

Commentary: This programme is to be replaced in 2013 by a new information sharing system authorised by section 81BA of the Tax Administration Act 1994. MSD expects that the new process will increase the likelihood of all student entitlements being paid correctly. In preparation for the new information sharing system with IR, the last match data received for this programme was in April.

Compliance: Compliant.

43 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.

2011/12 activity:

Match runs	50
Records received for matching	1,741,502
CSCs automatically renewed	205,451

'Invitation to Apply' forms sent out	91,696
Notices of adverse action	24,152
Challenges	136
Successful challenges	96

Commentary: Regulations defining how income is assessed, which affects eligibility for CSC, have not been updated by the Ministry of Health. Some cards may be issued to people who would not qualify if the regulations had been updated.

Compliance: Compliant with the information matching rules but not conforming to the purpose of the programme as cards are being issued to people who would not qualify.

44 IR/MSD (Netherlands) Tax Information Programme

Purpose: To enable income information about New Zealand-resident clients of the Netherlands government social and employment 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.

2011/12 activity: No requests for information were received from the Netherlands.

Commentary: Requests are normally received in June but the Netherlands have advised MSD that this year's batch is delayed. An audit on the operation of this programme found that there are effective controls in place and no issues were identified.

Compliance: Compliant.

45 MoE/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, first known study start date, end date (date of request), 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.

2011/12 activity:

Allowance applications

Records sent for matching (including repeat requests)	106,996
Individual applications involved in matching	76,754
Notices of adverse action	5,949
Successful challenges ⁸	2,278

Loan applications

Records sent for matching	14,454
Notices of adverse action	1,015
Successful challenges	205

Commentary: Challenges to adverse action notices are mostly resolved by the applicant providing clarification or updated information when contacted.

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.

46 Netherlands/MSD Change in Circumstances Programme

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

Year commenced: 2003

Features: Manual transfer of completed application forms as required.

MSD disclosure to Netherlands: MSD forwards the appropriate application

⁸ "Successful challenges" includes cases that are not eligible based on the initial match results, but are determined by StudyLink to be eligible after further investigation. In these cases no adverse action letter is sent.

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.

2011/12 activity: As an indicator of activity, MSD issued 829 notices of adverse action. This figure includes some corrections to SVB reference numbers. There were no challenges to these notices.

Commentary: MSD fixed the letter which advises clients of changes (s.103 notice) by restoring the warning that adverse action could occur as a result of the information match.

MSD also identified that people with an SVB number ending in '0' were not being sent s.103 notices. This system error has been corrected and notices have been sent to all who were affected.

Compliance: Compliant.

47 Netherlands/MSD General Adjustment Programme

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

Year commenced: 2003

Features: Data is transferred online four times each year.

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.

2011/12 activity: MSD made deductions from pension payments to 3,739 people. There were 1,233 MSD clients resident in the Netherlands.

Compliance: Compliant.

48 BDM(Deaths)/NPF Eligibility Programme

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

Year commenced: 2009

Features: Data transferred every four weeks by CD.

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

2011/12 activity:

Records received for matching	34,417
Possible matches identified - Pensioners	373
Possible matches identified - Contributors	85
Notices of adverse action sent	458
Challenges	0

Compliance: Compliant.

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

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

Year commenced: 2008

Features: Data transferred fortnightly by online transfer.

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

2011/12 Activity:

Match runs	26
Records received for matching	29,772
Possible matches identified	19,300
Notices of adverse action	11,826
Challenges	0
Successful challenges	0
Courtesy letters sent	5,430
Driver licence records cancelled	16,641

Commentary: Where NZTA intends to cancel a driver licence that is current or has expired within the last two years, it sends a notice of adverse action. For other cases, NZTA sends a courtesy letter advising the estate that the licence record is being cancelled.

Compliance: Compliant.

50 MoE/Teachers Council Registration Programme

Purpose: To ensure teachers are correctly registered (Teachers Council) and paid correctly (Ministry of Education).

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).

2011/12 Teachers Council activity:

Match runs	9
Average number records received from MoE in a match run	56,510
Matched, letter sent to establish registration status	3,815
Successful challenges	49
Not matched, letter sent	11
Match resolved by teacher response	10
Issues in process of being resolved	117
Number of matches confirmed by contact (cumulative)	3147

2011/12 MoE activity:

Number of teachers written to	465
Number of salaries adjusted	44

Commentary: The numbers not matched have dropped significantly, both through the operation of the match and as schools have improved their employment processes, perhaps in response to the match. The numbers of confirmed matches will continue to rise as the Teachers Council progresses through the register contacting teachers.

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 2012.



Privacy Commissioner

M Shroff

31 October 2012



General Manager

G F Bulog

31 October 2012

TO THE READERS OF OFFICE OF THE PRIVACY COMMISSIONER'S FINANCIAL STATEMENTS AND STATEMENT OF SERVICE PERFORMANCE FOR THE YEAR ENDED 30 JUNE 2012

The Auditor-General is the auditor of 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 99 to 124, that comprise the statement of financial position as at 30 June 2012, 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 92 to 98.

Opinion

In our opinion:

- the financial statements of the Privacy Commissioner on pages 99 to 124:
 - comply with generally accepted accounting practice in New Zealand; and
 - fairly reflect the Privacy Commissioner's:
 - financial position as at 30 June 2012; and
 - financial performance and cash flows for the year ended on that date.
- the statement of service performance of the Privacy Commissioner on pages 92 to 98:
 - complies with generally accepted accounting practice in New Zealand; and
 - fairly reflects, for each class of outputs for the year ended 30 June 2012, 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 31 October 2012. 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 preparation of the Privacy Commissioner's 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

STATEMENT OF OBJECTIVES AND SERVICE PERFORMANCE 2011/12

The work of the Office supports government priorities and justice sector outcomes to deliver greater prosperity, security and opportunities to all New Zealanders through safer communities. While the Office of the Privacy Commissioner is an Independent Crown entity and strongly maintains such independence, the work programme complements the government priorities of growing the economy and improving the quality of public services.

The Office works towards four long term outcomes. We currently measure progress at the output level.

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	3,248
Other Revenue	301	347
Total Revenue	3,449	3,595

STATEMENT OF OBJECTIVES AND SERVICE PERFORMANCE

FOR THE YEAR ENDED 30 JUNE 2012

	Actual 2012 \$000	Budget 2012 \$000
OUTPUT 1:		
Compliance		
Resources employed		
Revenue	1,477	1,417
Expenditure	1,430	1,423
Net Surplus(Deficit)	47	(6)
OUTPUT 2:		
Policy		
Resources employed		
Revenue	1,316	1,263
Expenditure	1,274	1,269
Net Surplus(Deficit)	42	(6)
OUTPUT 3:		
Information and Outreach		
Resources employed		
Revenue	470	451
Expenditure	454	452
Net Surplus(Deficit)	16	(1)
OUTPUT 4:		
International connections		
Resources employed		
Revenue	332	318
Expenditure	320	319
Net Surplus(Deficit)	12	(1)
TOTALS:		
Resources employed		
Revenue	3,595	3,502
Expenditure	3,478	3,463
Net Surplus(Deficit)	117	39

Output 1 – Compliance

- Handle complaints of interference with privacy;
- Monitor active information matching programmes.

Quantity	Estimation	Achieved 2011/12	Achieved 2010/11
Number of complaints received.	800 – 1,000	1142	968
Number of current complaints processed to completion or settled or discontinued.	800	1026	999
Projected number of active information matching programmes monitored.	53	50	47

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.	Not Achieved (2010/11 Not achieved 77.5%) Overall 76% of those who replied felt the process was satisfactory or better. The survey is of satisfaction with the overall quality of service, not satisfaction with the outcome. The scale is graduated from 1 'very dissatisfied' to 5 'very satisfied'. For the purposes of the survey options 3 to 5 have been treated as satisfied or above. 44% of complainants and 91% of respondents rated the process as satisfactory or better. Though the measure is satisfaction with the process it is anticipated that satisfaction is impacted for complainants by the nature of the final outcome. The response rate to the survey has been reducing over recent years and this may also have an impact on final figures.
Of the complaints processed, 30% are closed by settlement between the parties.	Achieved (2010/11 Not achieved) 311 of the 1,026 complaints processed were closed by settlement between the parties. (30.3%)
On 90% of the complaints closed we demonstrate personal contact, either by phone or in person, with one or more of the parties.	Not achieved (2010/11 Achieved) Achieved 81%. The increased number of complaints received impacts on achieving target of 90%. Goal being reassessed in line with continued growth in complaints workload. The result is difficult to report due to the data being collected being in the nature of exception reporting. New metadata will be introduced next year to record all instances of personal contact, providing definitive reporting.
Provide all draft reports on operating information matching programmes to the relevant departments for comment before they are published in the Annual Report.	Achieved (2010/11 Achieved) All relevant departments receive a draft report of their authorised information matching programmes for comment, prior to publication in the Annual Report of the Office of the Privacy Commissioner.

Timeliness	Achievement
80% of complaints are completed, settled or discontinued within 9 months of receipt.	Achieved (2010/11 Achieved 91%) 95% of complaints were completed, settled or discontinued.
Report on all operating information matching programmes in the Annual Report.	Achieved (2010/11 Achieved) Reports on all information matching programmes are published in the Annual Report of the Privacy Commissioner.

Output 2 – Policy

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

Improved management of privacy breaches within agencies.

Quantity	Achievement
Contribute to the Law Commission's Review of Privacy, providing comment and other contributions as requested.	Achieved (2010/11 Achieved) Law Commission Review completed in August 2011. Participant in public release of the Review.
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 (2010/11 Achieved) 115 new policy files created during the year in response to 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 with Department of Internal Affairs and Ministry of Health).	Achieved (2010/11 Achieved) Contact with departments as required under applicable memoranda of understanding. Formal reporting through the agreed Health work-plan. Internal Affairs has no detailed work-plan but regular meetings; substantial work was undertaken e.g. on Electronic Identification and Verification Service.

Quality	Achievement
Assistance provided to government agencies presents a clear, concise and logical argument, and is supported by facts.	Achieved (2010/11 Achieved) On-going 'Plain English' training received by the Policy team has also assisted clarity of communication.
Respond to feedback obtained from recipients of policy advice.	Achieved (2010/11 Limited actual feedback received) Feedback is sought on reports presented and it is through consultation and feedback processes that the final reports are developed.

Timeliness	Achievement
Advice given to agencies by the agreed date so that it is useful to them	Achieved (2010/11 Achieved) Despite sometimes very tight turn-around times being required of us by agencies.

Output 3 - 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 (2010/11 Achieved) Privacy Forum with nearly 250 attendees; UMR survey released; new poster "Time to Know Your Privacy Principles" very well received by privacy officers in agencies.
All media enquiries are recorded, logged and responded to within required deadlines.	Partly Achieved (2010/11 Partly achieved) The Office responded to 295 media enquiries. (2010/11 - 212) The deadlines for a media enquiry will vary according to the individual requirements of the enquirer; for this reason it is not possible to provide a defined deadline for measurement.
Provide assistance to promote better privacy practice in business and government.	Achieved (2010/11 Achieved) Including providing support for privacy officers; publishing posters; material on PSI site; new material on Business and Government website; disseminating case notes; running seminars such as Technology and Privacy Forums and the major Privacy Forum in May.
Provide an enquiries service including 0800 helpline and website access to information, supporting self-resolution of complaints.	Achieved (2010/11 Achieved 7,000 received) 8,468 enquiries were received.
Preparation of practical guidance materials to assist public awareness and understanding of the Privacy Act.	Achieved (2010/11 Achieved) Main product in this Financial Year was the 5 community advice cards, in partnership with Office for Senior Citizens (MSD) and Neighbourhood Support.
Maintain an effective website and other publications to assist stakeholders to promote better privacy practice.	Achieved (2010/11 Achieved) Website maintained. Website incorporates a Facebook page and Twitter account.

Activities	Estimation	Achieved 2011/12	Achieved 2010/11
Education workshops delivered.	30	47	37
Presentations at conferences/seminars	15	46	44
Projected number of enquiries received and answered.	6,000	8,468	7,000
Media enquiries received	250	295	212

Quality	Achievement
Seek out and act on feedback obtained from stakeholders and the public.	Achieved (2010/11 Achieved) This includes guidance material launched in August 2011 (developed from a senior citizens' focus group).
Evaluations show that the expectations of 90% of attendees at workshops were either met or exceeded for quality of presentation and materials.	Achieved (2010/11 Achieved) The overall percentage achieved is calculated as a percentage of the attendees and measure their expectations in coming to the workshop. 100% as having expectations being met or exceeded. 81% of attendees who completed the evaluation rated the presenter Very Good or or Excellent, while 78% rated the materials Very Good or Excellent. Less than 1% rated the presenter or materials Satisfactory or lower.
Case notes are published in accordance with standards adopted by the Asia Pacific Privacy Authorities (APPA) Forum.	Achieved (2010/11 Achieved) 13 case notes published. 11 case notes published during the year.
Website publications provide reliable and relevant information which is legally accurate and in plain English.	Achieved (2010/11 Achieved)

Timeliness	Achievement
Current information is placed on the website within 5 working days of being made available.	Achieved (2010/11 Achieved) Usually available same day or within 24 hours.
Response to 90% of enquiries within one working day.	Achieved (2010/11 Achieved 92%) 96% of enquiries were responded to within one working day.

Output 4 – International Connections

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

Support for economic growth through facilitation of the cross-border transfer of personal information

Quantity	Achievement
Participate in international forums.	Achieved (2010/11 Achieved) Participated in OECD Conference, Asia Pacific Privacy Authorities (APPA) Forum (2 meetings), International Conference of Data Protection and Privacy Commissioners, APEC Data Privacy Subgroup (2 meetings).
Contribute to international initiatives to facilitate cross-border cooperation in privacy standard setting and enforcement.	Achieved (2010/11 Achieved) Continued as Administrator of APEC Cross-border Privacy Enforcement Arrangement (CPEA) and as Committee member of Global Privacy Enforcement Network (GPEN). Participated in International Working Group on Privacy Enforcement Cooperation and Coordination. Initiated proposals to GPEN and International Working Group on enforcement coordination. Prepared a new GPEN Action Plan.
Monitor international privacy activities, codes and standards for their impact upon New Zealand's trade and investment opportunities.	Achieved (New measure in 2011/12) Continued participation in review of OECD Privacy Guidelines.
Quality	Achievement
New Zealand remains in consideration to achieve 'adequacy finding' from European Union.	Achieved (New measure in 2011/12) Consultation has continued with expectation that 'adequacy finding' will be achieved in the fourth quarter of 2012.
Participation is valued by peers and our contribution is influential.	Achieved (New measure in 2011/12) Continued in elected roles in CPEA and GPEN. Continued to receive speaking invitations to international events.
Timeliness	Achievement
Advice given to international jurisdictions by the agreed date so that it is useful to them.	Achieved (New measure in 2011/12) All deadlines are met.

STATEMENT OF ACCOUNTING POLICIES

FOR THE YEAR ENDED 30 JUNE 2012

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 2012, and were approved by the Commissioner on 31 October 2012. 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.

Funded Travel

The Commissioner and staff of the Office from time to time undertake travel at the request and cost of other agencies. These costs are not reflected in the Annual Report.

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.

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 2012:

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.

- Amendments to NZ IAS 1 Presentation of Financial Statements. The amendments introduce a requirement to present, either in the statement of changes in equity or the notes, for each component of equity, an analysis of other comprehensive income by item. CSE has decided to present this analysis in note 20.
- FRS-44 *New Zealand Additional Disclosures and Amendments to NZ IFRS to harmonise with IFRS and Australian Accounting Standards (Harmonisation Amendments)* – The purpose of the new standard and amendments is to harmonise Australian and New Zealand accounting standards with source IFRS and to eliminate many of the differences between the accounting standards in each jurisdiction. The main effect of the amendments on the CSE is that certain information about property valuations is no longer required to be disclosed. Note 14 has been updated for these changes.

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.

The Minister of Commerce has approved a new Accounting Standards Framework (incorporating a Tier Strategy) developed by the External Reporting Board (XRB). Under this Accounting Standards Framework, CSE is classified as a Tier 1 reporting entity and it will be required to apply full Public Benefit Entity Accounting Standards (PAS). These standards are being developed by the XRB based on current International Public Sector Accounting Standards. The effective date for the new standards for public sector entities is expected to be for reporting periods beginning on or after 1 July 2014. This means CSE expects to transition to the new standards in preparing its 30 June 2015 financial statements. As the PAS are still under development, CSE is unable to assess

the implications of the new Accounting Standards Framework at this time.

Due to the change in the Accounting Standards Framework for public benefit entities, it is expected that all new NZ IFRS and amendments to existing NZ IFRS will not be applicable to public benefit entities. Therefore, the XRB has effectively frozen the financial reporting requirements for public benefit entities up until the new Accounting Standard Framework is effective. Accordingly, no disclosure has been made about new or amended NZ IFRS that exclude public benefit entities from their scope.

STATEMENT OF COMPREHENSIVE INCOME

FOR THE YEAR ENDED 30 JUNE 2012

	Note	Actual 2012 \$000	Budget 2012 \$000	Actual 2011 \$000
Revenue				
Crown Revenue	2	3,248	3,148	3,148
Other Revenue	3	312	266	285
Interest		35	35	40
Total Income		3,595	3,449	3,473
Expenditure				
Promotion	4	49	53	38
Audit Fees		24	18	23
Depreciation and Amortisation	1, 10, 11	114	150	143
Rental Expense		401	402	398
Operating Expenses		371	391	430
Staff Expenses	5	2,508	2,449	2,441
Total Expenditure		3,467	3,463	3,473
Surplus/(Deficit)		128	(14)	0
Other comprehensive income		-	-	-
Total Comprehensive Income		128	(14)	0

STATEMENT OF CHANGES IN EQUITY

FOR THE YEAR ENDED 30 JUNE 2012

	Note	Actual 2012 \$000	Budget 2012 \$000	Actual 2011 \$000
Total Equity at the start of the year		528	430	528
Operating surplus for the period		128	(14)	0
Total recognised revenue and expenses for the period		128	(14)	0
Total Equity at the end of the year	6	656	416	528

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

STATEMENT OF FINANCIAL POSITION

AS AT 30 JUNE 2012

	Note	Actual 2012 \$000	Budget 2012 \$000	Actual 2011 \$000
Public Equity				
General funds	6	656	416	528
Total public equity		656	416	528
Current assets				
Cash & cash equivalents	7	469	349	606
Debtors and other receivables	8	16	75	9
Inventory		12	8	21
Prepayments	8	29	4	23
Total Current Assets		526	436	659
Non current assets				
Property, Plant & Equipment	10	306	208	225
Intangible assets	11	59	0	2
Total non-current assets		365	208	227
Total assets		891	644	885
Current liabilities				
Creditors and other payables	12	106	148	245
Employee entitlements	13	128	80	110
Total current liabilities		234	228	355
Total Liabilities		234	228	355
Net assets		657	416	528

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

STATEMENT OF CASH FLOWS

FOR THE YEAR ENDED 30 JUNE 2012

	Note	Actual 2012 \$000	Budget 2012 \$000	Actual 2011 \$000
Cash flows from operating activities				
Cash was provided from:				
Supply of outputs to the Crown		3,255	3,148	3,354
Revenues from services provided		312	266	65
Interest received		35	35	40
Cash was applied to:				
Payment to suppliers		879	864	888
Payments to employees		2,490	2,449	2,441
Net Goods and Services tax		116	15	(27)
Net cash flows from operating activities	14	117	1121	157
Cash flows from investing activities		-	-	-
Cash was provided from:				
Landlord's capital contribution		-	-	8
Cash was applied to:				
Purchase of Property Plant and Equipment		254	110	(24)
Purchase of Intangible Assets		-	-	-
Net cash flows from investing activities		-	-	(16)
Net increase (decrease) in cash held		(137)	11	141
Plus opening cash		606	338	465
Closing cash balance		469	349	606
Cash and bank		469	349	606
Closing cash balance		469	349	606

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 and accounting policies form part of these financial statements

STATEMENT OF COMMITMENTS

AS AT 30 JUNE 2012

	Actual 2012 \$000	Actual 2011 \$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	355
Later than one year and not later than five years	556	891
Later than five years	-	-

Other non-cancellable contracts

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

The Privacy Commissioner leases two properties, one in Wellington and the other in Auckland. The lease on the property in Wellington expires December 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 \$26,793 (2011: \$49,464)

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. (2011 \$nil)

STATEMENT OF CONTINGENT LIABILITIES

AS AT 30 JUNE 2012

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 (2011: nil).

NOTES TO THE FINANCIAL STATEMENTS

FOR THE YEAR ENDED 30 JUNE 2012

Note 1: Total Comprehensive Income

	Actual 2012 \$000	Actual 2011 \$000
The total comprehensive income is after charging for:		
Fees paid to auditors		
External audit	-	-
Current Year	24	23
Prior Year	23	21
Depreciation:		
Furniture & Fittings	62	63
Computer Equipment	40	26
Office Equipment	7	4
Total Depreciation for the year	109	93
Amortisation of Intangibles	2	50
Rental expense on operating leases	401	398

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

Crown Revenue

A Cabinet [CAB Min (11) 22/3] policy decision made on 10 June 2011. The Cabinet decision authorised an increase of \$100,000 a year in the annual appropriation to the Commissioner to enable it to manage its increased workload arising from the implementation of credit reporting (as introduced by sections 92A to 92H of the Summary Proceedings Act 1957, which came into force on 13 February 2012). Increased funds could not be confirmed at the time of budget preparation, in addition they were not received until April 2012.

Surplus

Unexpended revenue attributable to the increase in Crown Revenue and the appropriation of those funds held until April 2012.

Other Revenue / Operating Expenses

The Privacy Commissioner holds a Privacy Forum on a bi-annual basis. The Forum was held in May 2012 and produced revenues of \$40,000. Income was offset by an additional expense of \$21,000 incurred in hosting the Forum.

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 (2011 nil).

Note 3: Other revenue

	Actual 2012 \$000	Actual 2011 \$000
Other grants received	206	206
Rental income from property sub-leases	25	25
Privacy Forum	40	-
Seminars & Workshops	39	35
Other	2	19
Total other revenue	312	285

Note 4: Promotion expenses

	Actual 2012 \$000	Actual 2011 \$000
Website development expenses	2	10
Publications	17	-
Inventories consumed	-	7
Privacy Forum	21	-
Other marketing expenses	9	21
Total marketing expenses	49	38

Note 5: Staff Expenses

	Actual 2012 \$000	Actual 2011 \$000
Salaries and wages	2,353	2,288
Employer contributions to defined contribution plans	43	35
Other Staff expenses	25	39
Other contracted services	87	79
Total Staff Expenses	2,508	2,441

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

Note 6: General funds

	Actual 2012 \$000	Actual 2011 \$000
Opening balance	528	528
Net (deficit) / surplus	128	0
Closing balance	656	528

Note 7: Cash and cash equivalents

	Actual 2012 \$000	Actual 2011 \$000
Cash on hand and at bank	48	46
Cash equivalents – term deposits	421	560
Total cash and cash equivalents	469	606

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

Note 8: Debtors and other receivables

	Actual 2012 \$000	Actual 2011 \$000
Trade debtors	16	9
Prepayments	29	23
Total	45	32

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 (2011 \$NIL).

Impairment

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

Aging analysis:	2012 \$000	2011 \$000
Not past due	14	7
Past due 1-30 days	2	2
Past due 31-60 days		-
Past due 61-90 days		-
Past due >91 days		-
Total debtors and other receivables	16	9

As at 30 June 2012 no debtors have been identified as insolvent. (2011 \$NIL).

Note 9: Inventories

	Actual 2012 \$000	Actual 2011 \$000
Publications held for sale	12	21

The carrying amount of inventories held for distribution that are measured at current replacement cost as at 30 June 2012 amounted to \$NIL (2011 \$NIL).

There have been no write-down of inventories held for distribution or reversals of write-downs (2011 \$NIL).

No inventories are pledged as security for liabilities (2011 \$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 2010	561	191	116	868
Additions	2	23	-	25
Disposals	(148)	-	-	(148)
Balance at 30 June 2011	415	214	116	745
Balance at 1 July 2011	415	214	116	745
Additions	-	164	26	190
Disposals	-	(89)	(47)	(136)
Balance at 30 June 2012	415	289	95	799
Accumulated depreciation and impairment losses				
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
Balance at 1 July 2011	249	160	111	520
Depreciation expense	62	40	7	109
Elimination on disposal	-	(89)	(47)	(136)
Balance at 30 June 2012	311	111	71	493
Carrying amounts				
At 1 July 2011	166	54	5	225
At 30 June 2012	104	178	24	306

Note 11: Intangible assets

Movements for each class of intangible asset are as follows:

	Acquired software \$000
Cost	
Balance at 1 July 2010	283
Additions	-
Balance at 30 June 2011	283
Balance at 1 July 2011	283
Additions	62
Balance at 30 June 2012	345
Accumulated amortisation and impairment losses	
Balance at 1 July 2010	231
Amortisation expense	50
Balance at 30 June 2011	281
Balance at 1 July 2011	281
Amortisation expense	5
Balance at 30 June 2012	286
Carrying amounts	
At 1 July 2010	52
At 30 June and 1 July 2011	2
At 30 June 2012	59

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 2012 \$000	Actual 2011 \$000
Creditors	46	67
Accrued expenses	60	80
Other payables	-	98
Total creditors and other payables	106	245

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 2012 \$000	Actual 2011 \$000
Current employee entitlements are represented by:		
Accrued salaries and wages	3	7
Annual leave	125	103
Total current portion	128	110
Current	128	110
Non-current	-	-
Total employee entitlements	128	110

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

	Actual 2012 \$000	Actual 2011 \$000
Total comprehensive income	128	0
Add/(less) non-cash items:		
Depreciation and Amortisation	114	143
Other non Cash Items	-	-
Total non-cash items	114	143
Add/(less) movements in working capital items:		
Increase/(Decrease) in creditors	(21)	1
Increase/(Decrease) in accruals	(20)	2
(Increase)/Decrease in inventory	9	(11)
Increase/(Decrease) in payables	(98)	37
Increase/(Decrease) in employee entitlements	18	(7)
Increase/(Decrease) in Income in Advance	-	-
(Increase)/Decrease in receivables	(13)	
Working capital movements - net	(125)	22
Add/(less) items classified as investing activities:		
Landlord's capital contribution	-	(8)
Total investing activity items	-	(8)
Net cash flow from operating activities	117	157

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.

Marie Shroff (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 2011 there was a payment to the Trust of \$200 for membership fees) There are no commitments to the Trust at year end.

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 2012 \$000	Actual 2011 \$000
Total Salaries and other short-term employee benefits	870	859

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 2012	Actual 2011
\$100,000 - \$109,999		
\$110,000 - \$119,999		
\$120,000 - \$129,999		
\$130,000 - \$139,999	2	2
\$140,000 - \$149,999	1	1
\$150,000 - \$159,999		
\$160,000 - \$169,999	1	1
\$270,000 - \$279,999	1	1

Note 17: Commissioners' Total Remuneration

In accordance with the disclosure requirements of Section 152 (1)(a) of the Crown Entities Act 2004, the total remuneration includes all benefits paid during the period 1 July 2011 to 30 June 2012.

Name	Position	Amount 2012	Amount 2011
Marie Shroff	Privacy Commissioner	\$278,469	\$273,527

Note 18: Cessation Payments

No redundancy payments were made in the year. (2011 : 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:

	2012 \$000	2011 \$000
FINANCIAL ASSETS		
Loans and Receivables		
Cash and cash equivalents	469	606
Debtors and other receivables	16	9
Total loans and receivables	485	615
FINANCIAL LIABILITIES		
Financial liabilities at amortised cost		
Creditors and other payables	106	245
Total financial liabilities at amortised cost	106	245

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 2012 (2011: NIL). The Privacy Commissioner has no exposure to interest rate risk.

Liquidity risk

Liquidity risk is the risk that the Privacy Commissioner will encounter difficulty raising liquid funds to meet commitments as they fall due. Prudent liquidity risk management implies maintaining sufficient cash, the availability of funding through an adequate amount of committed credit facilities and the ability to close out market positions. The Privacy Commissioner aims to maintain flexibility in funding by keeping committed credit lines available.

In meeting its liquidity requirements, the Privacy Commissioner maintains a target level of investments that must mature within specified timeframes.

Market risk

Fair value interest rate risk

The Privacy Commissioner's exposure to fair value interest rate risk is limited to its bank deposits which are held at fixed rates of interest. The Privacy Commissioner does not hold significant interest-bearing assets, and have no interest-bearing liabilities.

The Privacy Commissioner invests cash and cash equivalents with the National Bank, ensuring a fair market return on any cash position, but do not seek to speculate on interest returns, and do not specifically monitor exposure to interest rate returns.

Cash flow interest rate risk

Cash flow interest rate risk is the risk that the cash flows from term deposits held at the National Bank will fluctuate because of changes in market interest rates. The Privacy Commissioner does not consider that there is any significant interest exposure on the Privacy Commissioner's investments. The Privacy Commissioner is primarily exposed to changes in the New Zealand Dollar Official Cash Rate.

Interest rate exposure – maturity profile of financial instruments

The following tables are based on the earlier contractual re-pricing or maturity period.

	Weighted average effective interest rate %	Variable interest rate NZ\$000	Fixed maturity dates – less than 1 year NZ\$000	Non interest bearing NZ\$000
2012 Financial assets				
Cash and cash equivalents	-	469	-	-
	-	469	-	-
2011 Financial assets				
Cash and cash equivalents	-	606	-	-
	-	606	-	-

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 2012 NZ\$000	Net surplus 2011 NZ\$000
Cash and cash equivalents +100 bps	4.90	3.25
Cash and cash equivalents – 100 bps	(4.90)	(3.25)

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

