A11

ANNUAL REPORT OF THE PRIVACY COMMISSIONER

For the year ended 30 June 2013

Presented to the House of Representatives

pursuant to section 24 of the Privacy Act 1993

November 2013

THE MINISTER OF JUSTICE

I tender my report as Privacy Commissioner
for the year ended 30 June 2013.

Marie Shroff
Privacy Commissioner

CONTENTS

CONTENTS

CONTENTS

CONTENTS

1: KEY POINTS

1: KEY POINTS

Communications

- We received over 9,000 enquiries from the members of the public and organisations seeking guidance on privacy matters.
- The Office received 310 media enquiries. Numbers were affected by the EQC incident and the MSD kiosk data breach, along with a steady stream of technology related enquiries.
- The Commissioner and senior staff gave 70 presentations and speeches during the year to a wide variety of audiences.
- The Office delivered 48 workshops and seminars to members of the public and stakeholder groups.
- During the year, we initiated a small ad hoc advisory group with participants from business, IT, academia and government, as recommended by the Law Commission. We held the first meeting in early April. We believe that the injection of perspectives will be helpful for a small agency like OPC in seeking to respond effectively to a very challenging environment.
- Pressure is continuing to affect our capacity to respond to rising external demands. Data breaches, government and business demands, media enquiries, new agreements for information sharing and the generally turbulent environment are placing a small agency like OPC under continual strain.

Complaints and investigations

- We received 824 privacy complaints from members of the public.
- The independent review of ACC's security of information was released in August 2012 (see http://www.acc.co.nz/news/WPC113544). The review found the breach of privacy of 6,748 clients was a genuine error, but it also highlighted systemic weaknesses within ACC's culture and processes.

Policy and technology

- We continued discussions with Ministry of Justice officials as they worked through the Privacy Act review proposals and look forward to the Government's response to that review shortly.
- The New Zealand Government's Bill to reform the Government Communications and Security Bureau (GCSB) took place against a background of heightened awareness and concern about government intrusion and surveillance of civilian life.

- Our submission on the GCSB Bill said that because of the complex and dynamic environment, we believe surveillance and in particular oversight of that activity needed to be considered further. We agreed that the law governing the GCSB's activities would benefit from additional clarity. (See: http://privacy.org.nz/news-and-publications/reports-to-parliament-and-government/government-communications-security-bureau-and-related-legislation-amendment-bill/) We recommended that a body such as the Law Commission be asked to investigate the most appropriate shape of the legislation to govern the intelligence agencies in New Zealand.
- Following the MSD kiosk incident in October 2012, the Government Chief Information Office (GCIO) was commissioned to review publicly accessible systems across government. The release of the GCIO's review in June 2013 (http://www.ssc.govt.nz/GCIO-publicsystemsreview) noted systemic privacy and security weaknesses across the public sector. The report included comprehensive recommendations. Key among the recommendations were new reporting and accountability measures for chief executives.
- Core government agencies are actively trying to do more with the data they hold, as part of the "Better Public Services" programme.
- The Information Sharing Bill became law in February 2013 and we received the first application for an approved information sharing agreement (AISA) a few months later. OPC must be consulted on each AISA, and can report on approved agreements. We will make our reports publicly available on our website to support transparency in government.

Data breaches

- Data breaches are being reported to us more frequently, and we have noticed a growing responsiveness by business and government to the reputational benefits of notifying clients when things go wrong. For the first time, we include a summary of these notifications later in this report.
- A number of public sector data breaches and security failures occurred during the year. In October 2012, journalist Keith Ng exposed security vulnerabilities in Ministry of Social Development (MSD) public-facing kiosks. The Deloitte report into that incident is available at: http://www.msd.govt.nz/documents/about-msd-and-our-work/newsroom/media-releases/2012/independent-review-deloitte.pdf
- In March 2013, EQC inadvertently released a document containing information about many tens of thousands of its Christchurch claimants.
- In addition, EQC had been struggling to respond to the huge numbers of information requests it was receiving from quake-affected Christchurch residents and had a large backlog.

- We had been in contact with EQC to try to assist them in managing this inflow and, together with the Ombudsman, are also engaged in the review of EQC's processes. EQC's experience showed very clearly how business processes and data management are entwined.

International

- A number of international privacy commissioners wrote a joint letter to Google chief executive Larry Page with specific questions about the nature and scope of the company's wearable Google Glass technology which is currently in development (See: www.privacy.org.nz). We received a response from Google which was broadly unsatisfactory and did not address the queries the commissioners raised. Together with our international colleagues, we are considering how to proceed on this issue.
- In early June, OPC participated in the Global Privacy Enforcement Network (GPEN) Internet Sweep which was an internationally coordinated effort to scan websites to assess the adequacy of their privacy notices and policies. We chose to focus upon particular target areas such as schools and children's websites. We released a summary of our findings. http://privacy.org.nz/news-and-publications/statements-media-releases/media-release-/
- The European Commission (EC) issued a long-awaited decision in December 2012 that New Zealand law is adequate for the purpose of European Union (EU) law which provides New Zealand businesses with a 'comparative advantage' in cross-border data processing. The decision came into effect across Europe in April 2013.

2: INTRODUCTION

2: INTRODUCTION

During the year, we started a small ad hoc advisory group with participants from business, IT, academia and government, as recommended by the Law Commission. We held an initial gathering in early April. We believe that the injection of perspectives will be helpful for a small agency like the Office of the Privacy Commissioner (OPC) in responding effectively to a very challenging environment.

Pressure is continuing to affect our capacity to respond to rising external demands. Data breaches, government and business demands, media enquiries, new agreements for information sharing and the generally turbulent environment are placing OPC under continual strain.

Law reform

Events during the year reinforced the need to ensure that OPC is equipped with tools to respond to the dynamic data environment that is developing across government and business. In the government context, having adequate privacy and security protections will enable the aims of Better Public Services to be realised successfully. We continued discussions with Ministry of Justice officials as they work through the Privacy Act review proposals. We expect the Government's response shortly.

ACC review

The independent review of ACC's privacy and security of information was released in August 2012 (see http://www.acc.co.nz/news/WPC113544). The report was commissioned jointly by OPC and the ACC Board following the unauthorised disclosure of details of 6,748 clients and had far-reaching recommendations for change. The review found the breach was a genuine error, but it also shows the error happened because of systemic weaknesses within ACC's culture, systems and processes.

The report showed that ACC lacked a comprehensive strategy for protecting and managing its client information. We noted at the time that a culture change within ACC was vital if further data security breaches were to be prevented.

Agencies that hold large amounts of personal information can take note of what has happened at ACC and have the opportunity to learn from its mistakes. Many organisations will recognise it could just as easily be them in the headlines.

Personal information is the lifeblood for organisations like ACC and it is vital that it treats that information with respect. The trust of its clients and, in many respects, the success of its operations depends on it. This sort of data is a major business asset with associated risks that have to be managed.

The review recommended that an independent audit of how ACC has implemented the changes is undertaken every two years and provided to the Privacy Commissioner. The review provided a strong set of proposals and we will monitor ACC's progress as it implements these changes.

MSD kiosk incident

The data security breach at ACC provided a timely warning to both public and private sector organisations, but it was to be followed by other high-profile data breaches and security failures. In December 2012, a security vulnerability in MSD's publicly-facing kiosks was exposed by the journalist Keith Ng.

EQC data breach

In March 2013, EQC had a data breach that involved many thousands of its Christchurch claimants. EQC has been struggling to respond to the huge numbers of information requests it is receiving from quake-affected Christchurch residents. We have been in contact with EQC to try to assist them in managing this inflow, and we and the Ombudsman are also engaged in the review of EQC's processes that is coming to a conclusion.

GCIO report

We noted the release in June of the GCIO's review of publicly accessible systems in government. The recommendations are significant and we hope will provide a platform for much needed change across government. One concerning aspect is our own limited resources, and the level and quality of suitable external consultants who are in a position to give quality advice and assist agencies. We are considering providing high-level, tailored training to key consultancies to help mitigate this, in discussion with key players.

NSA and PRISM surveillance

The revelations made by Edward Snowden in June 2013 made international headlines and sparked an ongoing debate about the scale and nature of government surveillance, and the surveillance activities of the US government in particular.

GCSB Bill

In New Zealand, the Government Bill to reform the Government Communication and Security Bureau arose against a background context of heightened awareness and concern about government intrusion and surveillance of civilian life.

Technology and international cooperation

Data protection and privacy commissioners are increasingly working collaboratively on issues of concern. This reflects the fact that the data practices of global businesses are having an impact across many jurisdictions, and the recognition that effective enforcement will often require international cooperation and coordination.

Google Glass

A number of international privacy commissioners wrote a joint letter to Google's chief executive Larry Page with specific questions about the nature and scope of

the company's Google Glass wearable technology currently in development (See: www.privacy.org.nz). The response from Google was broadly unsatisfactory and did not fully address the queries the commissioners raised. Together with our international colleagues, we are considering how to proceed on this issue.

GPEN Internet Sweep

In early June, OPC participated in the Global Privacy Enforcement Network (GPEN) Internet Sweep which was an internationally coordinated effort to scan websites to assess the adequacy of their privacy notices and policies. We chose to focus upon particular target areas such as schools and children's websites. We released a summary of our findings ("Websites leave children and parents guessing").

Information sharing agreements

The Information Sharing Bill became law in February 2013 and we received the first application for an approved information sharing agreement (AISA) a few months later. In an effort to establish the likely workflow, we contacted core government agencies and asked them to give an indication of proposed information sharing agreements. This revealed there may be a number of prospective agreements from the justice and health sectors among others.
OPC must be consulted on each AISA, and can report on approved agreements. Our plan is to make our reports publicly available on our website to support transparency in government.

European Union

The European Commission issued a long-awaited decision in December 2012 that New Zealand law is adequate for the purpose of EU law which provides New Zealand businesses with a 'comparative advantage' in cross-border data processing. The decision came into effect across Europe in April 2013. OPC assisted New Zealand Trade and Enterprise in May to deliver a workshop for business on EU data protection adequacy as part of NZICT's Tech Innovation Week.

The EU is in a process of replacing its data protection law. It has published a draft regulation which would, once adopted, replace all the data protection laws at national level across the EU.

The proposed law changes are substantial, will have a major effect on European privacy law and will indirectly influence approaches to privacy elsewhere. One direct effect on New Zealand will be on our existing 'adequacy' decision. How adequacy status will be recognised under the new regime has yet to be settled. One proposal is that adequacy decisions will continue until revoked or replaced by the EC. A counter-proposal for expiry after a set date could be contrary to New Zealand's interests and we have drawn this to the attention of MFAT. We will express concern at that approach with our European contacts and as opportunities arise, possibly in conjunction with other affected countries, such as Canada.

3. REPORT ON ACTIVITIES

3. REPORT ON ACTIVITIES

International activities

There is an increasing 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, cloud computing and off-shoring, individuals now publish, not just consume, content online. The Internet and mobile computing technology has made it easier than ever for individuals to post information about themselves and others literally to the world. This means global privacy enforcement authorities need to cooperate across borders to protect against privacy threats wherever they originate from. Collaboration with counterpart authorities can lead to enhanced problem solving, creative policy solutions and more effective regulation.

The Office engages 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 example, in the event of a security breach, we may need to seek the cooperation of offshore enforcement authorities;
- other countries may also encounter privacy challenges before they affect New Zealand.

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

- Asia Pacific Privacy Authorities (APPA) Forum: meets twice a year with a membership including authorities from Australia, Canada, Colombia, China, Korea, Mexico, New Zealand, Peru and the USA.
- International Conference of Data Protection and Privacy Commissioners: brings together nearly 100 Privacy Commissioners from around the world each year.
- 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) draws upon privacy expertise from across OECD countries to advance policy objectives.

Highlights

Some of the highlights during 2012/13 were:

- European Union: we continued our efforts towards securing a formal decision from the European Commission that New Zealand's law provides an 'adequate level of data protection' for the purposes of EU law. A positive decision was taken by the EC in December and came into effect in April. We released a document for businesses explaining the effect of the decision and worked with New Zealand Trade and Enterprise to run a workshop for businesses that might benefit from the new recognised status.
- OECD: we continued to assist the OECD Review of the 1980 Privacy Guidelines. The review successfully concluded during the year with the OECD Council adopting revised guidelines.
- Asia Pacific Privacy Authorities Forum: we participated in the 38th APPA meeting in San Francisco and agreed to host the 39th forum in Auckland in July 2013. The APPA Forum continues to build its reach in the region with two new members joining from South America.
- Global Privacy Enforcement Network: we continued to help lead the network through participation on the GPEN committee. We also worked to update GPEN's action plan to expand its capacity.
- APEC Cross-border Privacy Enforcement Arrangement: we continued as a CPEA administrator. This arrangement now connects 22 privacy enforcement authorities in seven APEC economies.
- APEC Data Privacy Sub-group: we participated in a DPS meeting in Jakarta and applied for approval from APEC's Committee on Trade and Investment to host a capacity building workshop for privacy enforcement authorities. Substantial preparations were undertaken during the year for this workshop which was held in Auckland shortly after the end of the reporting year.
- International Conference of Data Protection and Privacy Commissioners: we chaired a session at the 34th conference on the topic of enforcement cooperation and continued to serve on a working group devoted to enforcement coordination.

Information Services

Enquiries

We received over 9,000 individual contacts through our enquiries services – up from 8,500 the year before.

The service operates a 0800 phone line and an email address. As in previous years, the majority of enquiries were received by phone (about 75%). Email contact continued to increase with nearly a quarter of the contact through this channel.

Nearly a quarter of all contact was about disclosure or use of personal information. The next most common topic was enquiries about gaining access to information with around 1,600 contacts or a fifth of all contacts.

We don't attempt to gather demographic information from all the enquirers who contact us. Where appropriate, we record some details about enquirers or who they might represent. The largest group of contacts was from individuals, with over 7,000 (or about 78%) of all contacts. The next significant group of enquirers was people in the wider health sector at 613 contacts.

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 the previous years, there was a high demand from health sector agencies making up nearly 25% of the delivered sessions.

Feedback from all sessions showed that attendees were very satisfied with the training and that they found the content and trainers to be of a high standard.

Privacy Awareness Week (28 April to 4 May 2013)

Privacy Awareness Week is an annual event organised across Australia, Canada, Hong Kong, Macao, Mexico, New Zealand, South Korea and the United States by the Asia-Pacific Privacy Authorities (APPA).

The focus of Privacy Awareness Week 2013 was a half-day workshop, held in Wellington, on data breaches. A number of predominantly government agencies had experienced high-profile data breaches in the preceding months and the sessions were structured around how to avoid a major data breach and how to respond if you have one. We had speakers from organisations that had experienced data breaches and they told the audience what they had learned. The presentations are available on our website (www.privacy.org.nz).

We are developing an online Data Safety Toolkit, as a summary of the discussions and the practical strategies that participants identified.

Every year, APPA members collaborate on a joint product that can be used across the region. For PAW 2013, we designed a new infographic, "Technology is changing, but people still care about their privacy", that can be used as a poster, or put on an intranet or website (http://www.privacyawarenessweek.org/resources.html).

Other outreach

The Commissioner and her senior staff have given 70 speeches and presentations during the year on a range of topics and for a wide variety of audiences. Topics have included:

- Credit reporting code changes
- Big data
- Cloud computing and identity
- Auditing and data management practices
- Privacy law reform developments
- Managing data breaches in the public sector

Resource for schools

We are currently developing a primary schools' resource to teach children about privacy issues and the internet. The resource consists of 24 modules, with lesson plans, on different aspects of privacy that are relevant to children. The OWLS resource is being developed in partnership with NetSafe NZ, and with the assistance of the NZ National Commission for UNESCO.

Children often learn the hard way that privacy is important in today's digital world. Like the rest of us, they share information about themselves online, whether they are aware they are doing it or not. Taking control of information is important, but it's not always obvious how to do this, especially for younger students. The new resource aims to help students to be confident about how to manage their personal information and stay safe, so they can make the most of the online environment.

The OWLS resource recognises that schools, teachers and students will have varied experience and knowledge about how to handle personal information - from those with little access to technology to those who are already sophisticated and confident users. The modules that teachers can choose from are divided into four broad streams:

- **O**wn your information: take control of information about yourself.
- **W**ait and think before acting: take a moment to think about what you want to do.
- **L**ock your information: protect your information against people who want to steal it.
- **S**afety: avoid some major risks, and have back-up plans if things go wrong.

We hope the OWLS modules will also provide ways for students and teachers to involve families and whanau, and wider communities.

Media

Enquiries from the media continued to flow in on a wide range of personal information and technology topics. The Office received 310 media enquiries during the year. This is the second highest number we have received, close to our highest total of 323 in 2009/10.

The release of the ACC report, and numerous other data breaches across the public sector, including EQC and the MSD kiosk issue, contributed strongly to the media enquiries we received. Employee browsing of client records, such as Jesse Ryder's records; the GCSB report and Bill; the use of drones, and automatic number plate recognition, are a few of the areas that also generated interest.

The vast majority of media enquiries arise from externally generated events, rather than from Office media releases.

Our capacity to respond to media requests for comment, or to assist in providing background information, has been stretched with no full-time communications staff. Other staff, particularly those in the policy and technology areas, often contribute in responding to media queries. The extended demand for assistance in this area led us to address this at the end of the year by appointing a full time communications adviser.

Complaints and access reviews

We received a total of 824 complaints in the 2012/13 year. Table 1 shows incoming and closed complaints and work in progress at year's end. Work in progress returned to more usual levels after a number of high profile data breaches from March 2012 onwards had been dealt with.

TABLE 1: COMPLAINTS RECEIVED AND CLOSED 2008-2013

	2008/09	2009/10	2010/11	2011/12	2012/13
Complaints received	806	978	968	1,142	824
Complaints closed	822	961	999	1,026	896
Work in progress after year's end	273	290	247	363	291

The complaints process

The complaint process aims, in the first instance, to gather sufficient information to allow us to form a view that a complaint has substance. In most cases, we look for circumstances that indicate a breach of the Privacy Act and which show some harm to the individual who is the subject of the breach. Where we believe that there is substance to a case, we will attempt to motivate the parties to resolve the complaint. Where sufficient harm is not demonstrated in the complaint, it is unlikely that we will continue or complete an investigation.

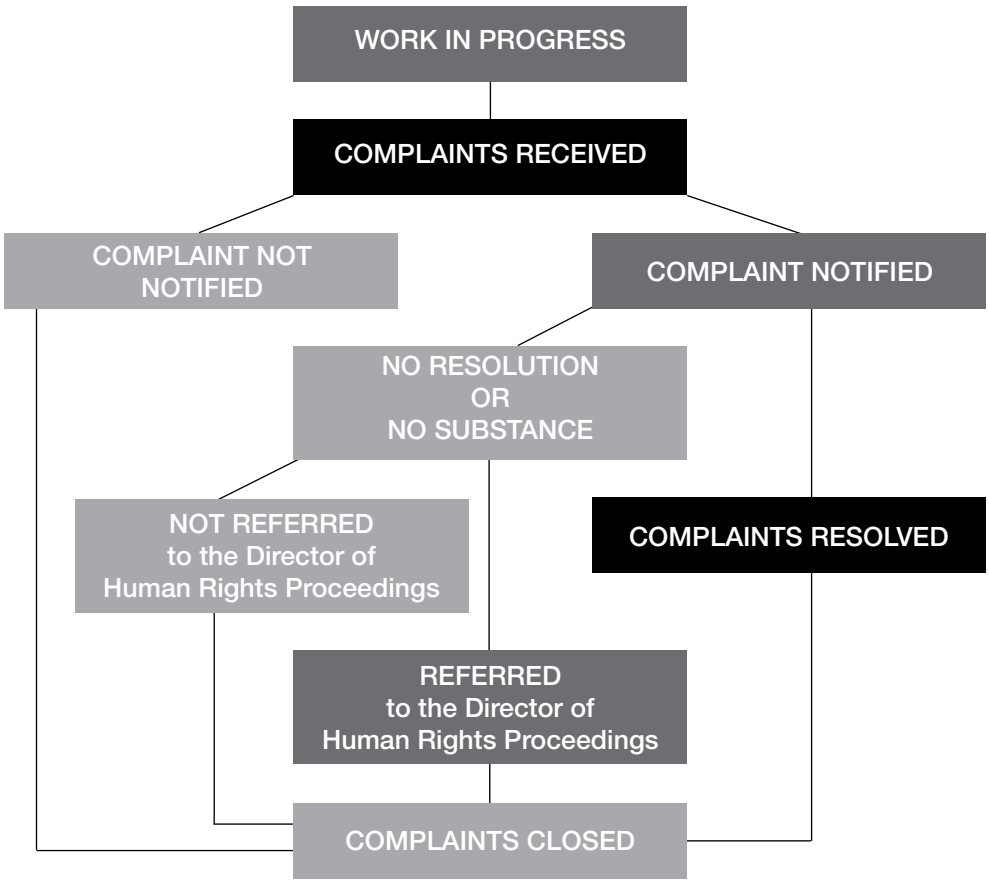
We also assess complaints for systemic issues that raise wider or general concerns for the community at large. Where an individual complaint may not have

substance but contains systemic practices that may impact on a wider section of the community, we may undertake an investigation into that practice or system on our own initiative. For example, this year an individual complaint motivated us to look at how a government agency displayed registration information about individuals online. With input from us, the agency has modified its practices to allow for increased privacy on the internet version of its records.

Figure 1 shows the breakdown of outcomes for complaints closed during the 2012/13 year. The complaints 'not notified' were either issues that we considered at an early stage had no substance or, after initial contact, the complainant failed to pursue the complaint. Complaints that were notified progressed through the complaints process and were resolved or on further investigation were found not to have substance. A complaint that had substance and could not be resolved might also warrant referral to the Director of Human Rights Proceedings.

Overview 2012/13

FIGURE 1: COMPLAINTS AND ENQUIRIES PROCESS



Our aim is to settle 30% of all complaints. Settlement outcomes for this year are shown in Table 2. Of the complaints closed for the year 2012/13, 36% were closed with some level of settlement. This was an increase on our settlement rate from last year. We achieved some level of resolution in nearly 63% of the complaints that were notified.

Settlements range from apologies through to payments of money for harm caused. Monetary compensation was generally for amounts less than $5,000, with some greater than $10,000.

The total number for outcomes listed in the table is higher than the number of complaints settled as some complaints had multiple settlement outcomes - such as an apology, assurances and a monetary payment.

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 2012/13

Settlement outcome	Number
Information released	104
Apology	68
Money/monies worth	21
Information partly released	31
Information corrected	36
Assurances	105
Change of policy	55
Training	0

Personal contact

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

This year, we had personal contact with one or more of the parties to a complaint on 69% (622) of the complaint files

Complaints received

Past trends continued to be reflected in the incoming complaints for the year. Of the 824 complaints received, over 70% were for alleged breaches of privacy under the Act's information privacy principles. Table 3 shows a breakdown between the privacy principles and rules contained in the three privacy codes. About 60% of the complaints received were from individuals asking us to review the results of access requests they have made to agencies.

TABLE 3: ACT/CODE – BREAKDOWN OF COMPLAINTS RECEIVED 2012/13

Information Privacy Principle	628
Health Information Privacy Code	183
Telecommunications Privacy Code	9
Credit Reporting Code	4
Not identified in category	0
TOTAL	824

Agency types

Table 4 provides a breakdown of complaints in various sectors. The three major categories of government, health and financial sectors comprise nearly 60% of our complaints, with complaints about the public sector (37%) being the biggest overall segment.

TABLE 4: COMPLAINTS RECEIVED BY AGENCY TYPE 2012/13

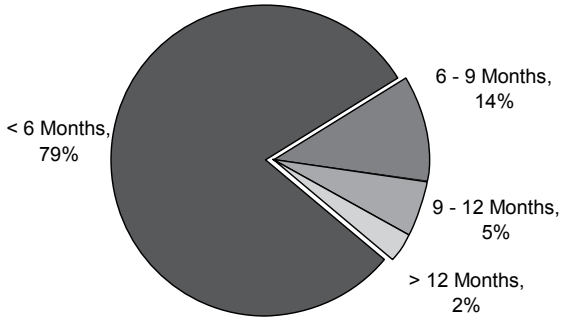
Agency Type	Total	Percentage
Government sector, including education and local authorities	304	37%
Health sector, including hospitals and medical practices	112	14%
Financial sector, including banking, insurance, credit agencies and debt collectors	54	7%
Other	354	43%
Total	824	100%

Age of complaints

Each year, we aim to complete no less than 80% of our complaint investigations within nine months of receipt. Figure 2 demonstrates that we achieved our desired outcome by closing 93% within nine months. The remaining 7% mostly involved protracted settlement issues.

At year's end, work in progress totalled 294 files of which 89% were under nine months old.

FIGURE 2: AGE OF CLOSED COMPLAINTS 2011/12



Top respondent agencies

This year, eight agencies generated more than 10 complaints each to the Privacy Commissioner. Non-government agencies have not made the top respondent list for the past five years.

Table 5 sets out the complaints received and the number closed throughout the year for top respondent agencies. In total, these agencies were responsible for almost 40% of the Privacy Commissioner's complaints work.

TABLE 5: COMPLAINTS RECEIVED AND CLOSED FOR TOP RESPONDENT AGENCIES 2012/13

Agency	No of complaints received	No of complaints closed
Accident Compensation Corporation	79	186
Ministry of Social Development	61	53
New Zealand Police	51	47
Department of Corrections	45	52
Department of Labour (Immigration New Zealand)	32	27
Government Communications Security Bureau	19	3
New Zealand Security Intelligence Service	13	11
Housing New Zealand	11	10
TOTAL	311	389

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

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

A complaint outcome of "no interference with privacy" is where we considered there had been no privacy issues that needed a response. A complaint that has some substance involves a matter where some rectifying response was required by the agency. Some of the cases with substance will have a mixture of issues and not all require attention by the agency. For example, on a review of an access case, we may recommend that more information be released to the requestor, while agreeing with the agency that some information can be withheld on proper grounds. The outcome of a complaint that has substance may range from the release of further information, through to an apology and compensation for damages for wrongful collection or disclosure of personal information.

The Accident Compensation Corporation figures reflect the aftermath of the March 2012 data breach incident. The settlements ranged from those who were satisfied with the recommendations that came out of the independent investigation into ACC's handling of the data breach, through to those who had suffered significantly as a result of the breach. The majority of settlement outcomes were in the first group.

TABLE 6: OUTCOMES FOR TOP RESPONDENT AGENCIES 2012/13

Agency	Closed	No interference with privacy	Complaint has some substance	Settled/ mediated	Referred to Director of Human Rights Proceedings
Accident Compensation Corporation	186	56	130	130	0
Ministry of Social Development	53	44	9	9	0
New Zealand Police	47	35	12	12	0
Department of Corrections	52	35	17	16	0
Department of Labour (Immigration New Zealand)	27	14	13	13	0
Government Communications Security Bureau	3	2	1	1	0
New Zealand Security Intelligence Service	11	9	2	2	0
Housing New Zealand	10	8	2	2	0
	389				

Satisfaction survey

Each year, we measure our complaint service through a satisfaction survey. Every complainant and respondent received a satisfaction survey with our closing letter, and a prepaid envelope. The survey is completed anonymously.

This year, we received 138 completed responses – 88 from complainants and 50 from respondents. This represents about an 8% response.

The survey questions were the same as previous years. Participants were asked to rate the various factors on a scale of 1 to 5, with the lower numbers reflecting negative comment and the higher numbers reflecting positive comment. We calculate a score of three or better as being satisfied, through to a score of five being very satisfied. The survey results were:

- 70% said they were satisfied or very satisfied with the service (complainants 50% and respondents 90%)
- 89% had expectations of a good to very good service
- 78% felt their expectations were met or bettered (complainants 58% and respondents 98%)
- 82% agreed or strongly agreed that staff were competent (complainants 65% and respondents 100%)
- 85% agreed or strongly agreed that staff kept their promises (complainants 71% and respondents 100%)
- 78% agreed or strongly agreed that they were treated fairly (complainants 65% and respondents 91%)
- 66% agreed or strongly agreed that individual circumstances were considered (complainants 48% and respondents 85%)
- 74% agreed or strongly agreed that the service was good value for taxpayer money (complainants 51% and respondents 96%)

External audit

This year, we again contracted a barrister experienced in privacy issues to audit a random selection of 20 complaint files to determine the quality of our investigations process. The barrister assessed aspects such as analysis of legal issues, clarity and sensitivity of communications and correspondence, and fairness and timeliness of the process. A new field was also included assessing the efficiency of the complaints 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 76.25. The average file score was 3.8 out of five. This is a lower total than in previous years and possibly a reflection of a new barrister's view of the files. However, the total score and average are still within acceptable levels of performance on all files.

Litigation

The enforcement scheme of the Privacy Act

An essential part of any privacy regulation is the ability to enforce the law in appropriate cases. Enforcement provides incentives for agencies to comply with the law. Agencies that do not comply with the law can be held to account, usually in a public forum. They can be ordered to change their ways and, if necessary, to compensate individuals for the harm that they have caused. Enforcement action also provides guidance for other agencies about what the law means and how to manage personal information successfully.

The Privacy Commissioner currently does not have any direct enforcement powers, such as an ability to make enforceable orders, although this would change under the reforms proposed by the Law Commission. The Privacy Commissioner's role is essentially recommendatory. In fact, however, the statutory scheme of the Act allows the Commissioner to put appropriate matters on a litigation track and this has become a routine part of the Office's work.

Most complaints are resolved during the course of our complaint investigation. But there is always a small proportion of complaints that are not resolved and in which litigation may be necessary or desirable. The Human Rights Review Tribunal is the specialist judicial body to which those cases can be brought.

The process through which cases get to the Tribunal

There are two ways in which a privacy complaint may reach the Tribunal. First, the complainant can file proceedings in the Tribunal on their own account if we form the view that there is no substance to the complaint or decide not to take further action. Secondly, if we form the view that there is substance to a complaint but the parties are unable to achieve a settlement, we can refer the complaint to the Director of Human Rights Proceedings (a separate statutory authority) who makes an independent decision about whether to bring proceedings against the agency in the Tribunal.

We occasionally act as an intervener in Tribunal proceedings. Our role is to act as an expert adviser to the Tribunal about the interpretation of the law. This year, we participated in five Tribunal hearings.

Referral to the Director is normal practice

It is our standard practice to refer a matter to the Director when we think there is substance to a complaint but where the parties do not settle. Often in these

cases, our view will be that the agency is at fault and the matter needs to be put before the Tribunal for formal resolution. Less commonly, but also importantly, it is appropriate to refer a complaint when the meaning of a provision in the Act is unclear and where a decision from the Tribunal will provide greater certainty about how the Act operates.

It is only on rare occasions that we decide it is inappropriate to refer. Instances where we have not referred a case have included situations where the complainant's circumstances make it inappropriate or difficult for them to be a witness; where the agency has engaged its best endeavours to settle but where the complainant has unrealistic expectations; or where the issues are minor in nature and it would be disproportionate to engage further state-funded resources to resolve them. If we decide not to refer, the complainant can still take proceedings on their own account.

The increasing trend to litigate following own motion investigations

It is not only complaint files that can be referred to the Director to consider filing proceedings. It is increasingly common for us to conduct own-motion inquiries and to seek assurances from the agency against repetition of behaviour. For example, if it is our view that an agency is failing to secure personal information properly, we can seek assurances that it will amend its security standards in particular ways. If the agency does not provide those assurances, we will refer the matter to the Director.

An analysis of litigation statistics

As Table 7 shows, the number of referrals to the Director declined in the last couple of years and the number of privacy cases in the Tribunal has also declined this year. It is too early to tell whether this is a trend or merely a quiet patch, but there are indications that agencies are choosing to change their processes rather than put matters on a litigation track.

For instance, agencies are now well aware that if settlement is not forthcoming in appropriate cases, they are likely to face the prospect of litigation with all that that entails (including time, trouble, cost and publicity). This has resulted in agencies being more willing to settle appropriate cases.

Another influential factor is likely to be the increased level of compensation that the Tribunal is prepared to grant in cases where a breach of the law has caused harm to an individual. There have been several awards of between $10,000 and $20,000 – a level that provides a stronger financial incentive for agencies to resolve disputes voluntarily.

Possible law reform

The Law Commission has made several recommendations that would affect OPC's enforcement role. First, it recommended that OPC should be able to order agencies to release information in response to access requests, and should be able to also order agencies to comply with the privacy principles. Those orders would be legally enforceable. Agencies could appeal to the Tribunal if required. Secondly, the Law Commission recommended that OPC should be able to take cases directly to the Tribunal rather than having to refer cases to the Director for consideration. We support these recommendations, as they would eliminate duplication and confusion for the parties, and make the enforcement processes quicker and more efficient. They would also make the OPC directly accountable in the Tribunal for the decisions that we reach.

Other litigation

We were a defendant in one judicial review proceeding this year (*Siemer v Privacy Commissioner and Official Assignee*), and successfully defended the claim. We were also named as a respondent in Employment Court proceedings (*Aarts v Barnardos et al*). The claim was struck out. (At time of writing, the plaintiff is applying for leave to appeal to the Court of Appeal).

TABLE 7: REFERRALS, TRIBUNAL CASES AND OUTCOMES 2007-2013

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

At year end, the Director was considering whether to take proceedings in 13 cases. He settled one complaint during the reporting year, declined to take proceedings in five instances (mostly files that were referred to him some time ago), and filed proceedings in one case.

The Tribunal awarded compensation in each of the cases in which it found an interference with privacy had occurred. The awards were $10,000 damages *(Fehling v South Westland School)*; $20,000 damages and $3,500 costs to the Director *(Director of Human Rights Proceedings v INS Restoration Ltd);* $20,000 damages and $7,500 costs to the Director *(Director of Human Rights Proceedings v Hamilton)*; total of $17,000 damages – but reduced on appeal to the High Court to $2,000 *(Holmes v Ministry of Social Development)*.

Breach notifications

We have recently started to track breach notifications more formally, as this is a growing body of work for the Office and is also a matter of external interest and importance.

We are still developing our reporting system, including considering the most accurate and useful way of reporting types of breaches and outcomes. Provisional figures since our record-keeping began part way through 2007 are as follows:

TABLE 8: NUMBERS OF NOTIFICATIONS AND SECTOR

Year	Total Notifications	Public sector	Private sector
*07/08	3	2	1
08/09	16	13	3
09/10	13	10	3
10/11	31	19	12
11/12	46	34	12
12/13	107	84	23

*partial year results only, dating from the switch to the electronic records system in August 2007.

TABLE 9: MOST COMMON SECTORS FOR NOTIFICATIONS

Organisation type	07/08	08/09	09/10	10/11	11/12	12/13
Government	2	7	9	15	27	51
Hospital	0	5	1	3	5	12
Other health agencies	1	0	2	3	2	6
Large businesses (general)	0	1	0	3	3	7
Education sector	0	1	0	1	1	4
Small businesses	0	2	0	2	2	5
Local authorities	0	0	0	0	0	3
Banking/Finance/Insurance	0	0	0	3	3	4
Telecommunications	0	0	1	0	2	3

The figures represent the number of notifications received (not the numbers of agencies that notified us).

TABLE 10: MOST COMMON TYPES FOR BREACHES NOTIFIED

Types of breach	07/08	08/09	09/10	10/11	11/12	12/13
Website problem		3		2	2	12
Loss/theft of physical file	1	5	4	2	7	5
Loss/theft of portable storage device		1	3	1	5	7
Employee browsing		1		1	3	6
Electronic information sent to wrong recipient	1	2		2	10	17
Physical information sent to wrong recipient		2	3		5	23
Hacking				4	1	4

The figures demonstrate that our own workload with breaches has increased markedly in the last year. This is unsurprising, given the major data breaches at ACC and MSD. Not only public sector agencies have a heightened awareness of breach reporting. Private sector reporting is also significantly up. We are receiving notifications from a greater variety of sectors, indicating that awareness of breach notification best practice is becoming more widespread.

It is too early to say whether our statistics illustrate a trend, or merely a temporary rise in concern. But we would be surprised if reporting was to diminish much in the near future. Experience overseas suggests that breach numbers are increasing significantly, particularly as agencies apply new technologies in ways that test the maturity of their security safeguards. Local agencies are likely to maintain their heightened awareness of breach prevention and management for some time to come.

As mentioned, these figures are still provisional. They should be approached with a degree of caution.

Firstly, breach reporting is entirely voluntary in New Zealand at present. This means that our figures say little about the level of breaches that actually occur, or the relative performance of agencies in various sectors. Instead, the agencies that report to us tend to be the conscientious ones that are able to identify breaches when they occur and that are well aware of best practice in breach reporting. That is, they know that they should generally notify the individuals concerned and also our office where there has been a serious breach, or where notification will help the individual to take steps to protect themselves. Most agencies that contact us are also aware of our voluntary privacy breach guidelines and are already following them.

Secondly, there is no formal definition of what amounts to a breach. As a result, some of the breaches are minor issues that would not be required to be notified under any mandatory scheme. The figures alone therefore do not necessarily tell

us whether an agency has a serious issue with its security standards. In addition, a few notifications involve agencies that have discovered that their disclosure processes may breach the Act. Not all of these are "data breaches" as we would often understand the term. Data breaches more usually involve either deliberate misuses or theft of personal information (such as employee browsing, hacking, or theft of data storage devices), or inadvertent actions by an agency that expose personal information. For simplicity's sake, we currently log all voluntary notifications from agencies as breaches.

We encourage agencies to let us know when they experience a breach. We can often provide useful advice on how to handle the breach, particularly for those with little experience in the area. If the agency is already doing everything that we recommend, they feel reassured. In cases where follow-up is warranted, we can often provide an early indication of what we are likely to need - an approach which is easier for the agency to manage than receiving a formal notification of an enquiry. Finally, if a breach results in significant publicity, we are better equipped to take enquiries from individuals who are or may be affected, and to provide information in response to media enquiries.

The Law Commission has recommended that New Zealand needs to move to mandatory breach reporting. We agree with that recommendation. Mandatory reporting would provide strong incentives for agencies to take appropriate steps to prevent breaches and to manage them properly when they occur. It would result in better information being given to affected individuals so that they could take steps to protect themselves. It would provide us with better information about the scale of the breach problem in New Zealand, the types of breaches that occur, and what approaches are effective. This would give us information that we can then use to help others. It would also provide a direct mechanism for us to deal with agencies that do not attempt to comply or refuse to comply with the law, allowing us to target our responses to greatest effect to protect individuals from harm.

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. However, it is a power that we exercise with considerable care.

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. One is not yet formally concluded. Details of the other applications are as follows:

Application by credit reporter to allow disclosure where an agency's clients are "gone: no address"

Veda Advantage applied for an exemption to allow it to disclose information to two investment companies. Between them, the companies had 47,000 clients with whom they had lost touch, and to whom they had payments to make. The companies were trying to get new contact information for those clients and had been unsuccessful using other methods of tracing.

We recognised that if Veda did hold information about these clients, that there would be a benefit to them (they would receive money that was owed to them). However, on balance, we declined the application. Our reasons included:

- The section 54 power is not intended as a way to allow the Commissioner to circumvent Parliament's intention and to change how the Act operates. Any change should be done via a properly consulted Code of Practice. The Credit Reporting Privacy Code does not currently allow for credit reporters to use information in this way
- The inability to contact people who are "gone: no address" is not a one-off incident. It is an ongoing issue that affects other investment companies (and similar bodies) and other credit reporters. It should be dealt with in a systematic way
- If the exemption were permitted, Veda would receive information about 47,000 individuals without those individuals being aware of the fact – the individuals would not be aware of their rights under the Credit Reporting Privacy Code
- The information received by Veda could be used for future credit reporting purposes, again without those individuals being aware of it.

While the application was unsuitable for a section 54 exemption, the issue of tracing people who are "gone: no address" is likely to be discussed when the Credit Reporting Privacy Code is reviewed.

Shared library services

Tasman District Council applied for an exemption to allow it to disclose information from its database of library users to Nelson City Council, to allow those users to access libraries in both areas.

We recognised the potential benefits for library clients, and for Councils, in developing shared library services. However, we believed that the application was premature and we declined it. Our reasons included:

- The application proposed the transfer of full records about existing library clients, including information about their borrowing history, and library charges incurred (both historical and current). As a result there were some potential sensitivities for library clients.

- Users could currently apply for access to the other Council's libraries. Application forms stated what was to be done with the users' personal information asked for consent in the normal way.
- We had insufficient information to be able to properly assess the public interest in the proposal. We had no indication of how many people were likely to want to take up the offer, and the financial savings for the Councils were not quantified.

The Councils are apparently considering a plan for a shared library service. We believed that issues relating to records of existing customers would be better dealt with as part of that plan.

Policy

OPC'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
- providing privacy advice to the private and public sectors on new technology issues, including by producing guidance
- providing advice to 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 is intended to ensure that government and Parliament take into account the potential impacts on New Zealanders' privacy when they create new laws.

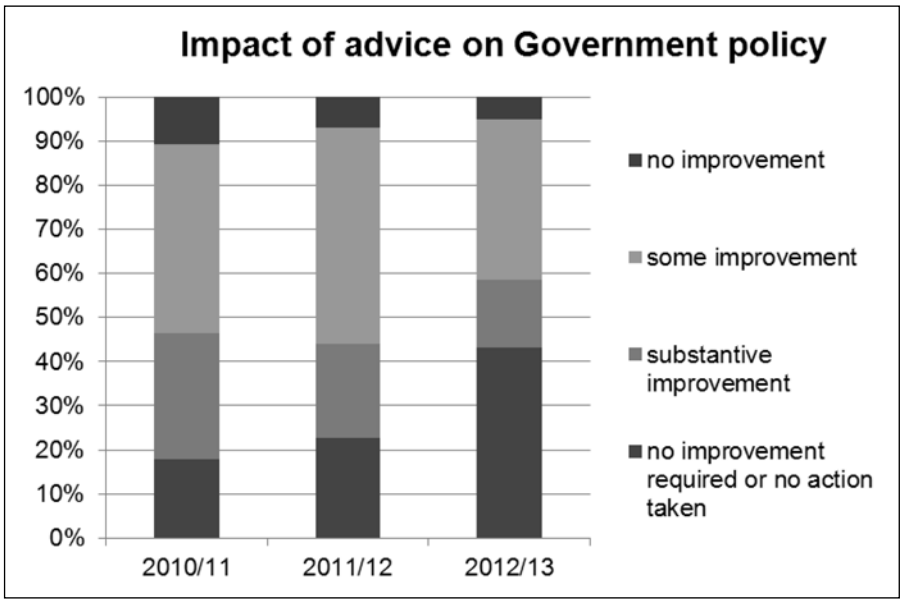
We assess the impact of our advice by whether we are able to achieve changes to legislation before it is passed. We are also seeking to reduce the proportion of files requiring the Office to intervene by encouraging agencies to undertake deeper privacy analysis before approaching us.

We assessed the impact of our advice on 58 policy files:

- 57% raised privacy issues that we considered needed further attention (down from 77% in 2011/12)
- 91% of files requiring further consideration saw some improvement as a result of our advice (the same as 2011/12)

- 27% were "substantively improved" (unchanged from 2011/12).[1]

FIGURE 3: IMPACT OF ADVICE ON GOVERNMENT POLICY



Since 2010/11, we have seen a reduction in the number of files that raise privacy issues requiring our attention. However, there is a need to apply caution to these figures because there are only two years of complete data and the number of files considered is relatively small. We judge that the reduction in the number of files requiring attention is due to a range of factors, in particular:

- stronger relationships with key government departments and agencies and clearer understandings of our expectations with regard to privacy
- increased awareness of privacy issues, particularly in the wake of high profile privacy breaches in the public sector
- a small increase in the number of files provided to us 'for information' after key decisions have been taken and the opportunity to influence policy has passed.

While the last of these points can be interpreted as a negative development, the files we received that fell into this category would not have been presented to the Office at all in previous years. It should therefore be seen as part of the wider trend of stronger relationships, and greater public sector awareness of privacy.

In coming years, we will be working to embed privacy thinking into government departments' policy processes with the aim of increasing the number of files that do not require advocacy by the Office.

1 Note that the method of calculation of some figures differs from that in the 2011/12 annual report. 2011/12 figures have also been revised to reflect assessments made in 2012/13 about work undertaken in the 2011/12 financial year.

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

- support for government efforts to improve personal information management in the public sector in response to the GCIO Review of Publicly Accessible Systems and high profile breaches at ACC and MSD
- implementation of the Green Paper on vulnerable children
- the Social Security (Benefit Categories and Work Focus) Amendment Act 2013
- implementation of the Privacy Amendment Act 2013 on information sharing
- development of the Ministry of Education's systems for managing information on children in Early Childhood Education
- the Social Housing Reform Bill
- the GCSB Amendment Act 2013
- the planned Organised Crime and Anti-Corruption Bill.

We have also continued to contribute to the Ministry of Justice's work on reform of the Privacy Act in response to the Law Commission's report.

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 specifically.

During 2012/13, the OPC continued to provide advice to the National Health IT Board on electronic health records (EHRs). A major initiative during the year has been the review of three EHR initiatives. Our reporting on this review will be released later in 2013. 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 practices in the private sector are 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 helpful and timely advice.

In February, we launched guidance aimed at small and medium enterprises considering whether to use cloud computing services as part of their businesses. This guidance was well-received by the cloud computing industry, and has been

used by a number of organisations as a guide to the information they need to provide to potential customers.

Information matching and sharing

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.

In February 2013, Parliament passed the Privacy Amendment Act 2013. This Act allows government departments to agree to share personal information in order to provide public services when that sharing agreement is authorised by an Order in Council. Before seeking an Order in Council, departments must consult the Privacy Commissioner. The Commissioner also has the power to report to the responsible minister on an agreement and publish that report, to specify reporting, and to seek reviews. No agreements had been approved in the 2012/13 year. The first approved information sharing agreement was finalised shortly after the end of the reporting year.

Codes of practice

At the start of the year, there were five codes of practice in force. During the year, the Civil Defence National Emergencies (Information Sharing) Code was issued and two existing codes were amended.

Civil Defence National Emergencies (Information Sharing) Code

In 2011, the Privacy Commissioner issued the Christchurch Earthquake (Information Sharing) Code within 48 hours of the 22 February 2011 earthquake. The code was a precaution to ensure that the agencies involved in responding to the emergency, and other agencies interacting with them and with the victims' families, had sufficient authority to share personal information as needed. The code was temporary and expired after about four months.

Prior to its expiry, the Office reviewed the code's usefulness with its stakeholders and 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 faced another national emergency. Accordingly, we publicly notified a proposed code in 2012 and took public submissions. The proposed code, like the temporary Christchurch code, would supplement the existing law and provide additional authority to collect and disclose personal information. It would provide that in addition to any existing lawful reason for disclosure, 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 provided that a permitted purpose included:

- identifying individuals who are or may be injured, missing or dead as 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; and
- ensuring that responsible people (such as parents, spouses, partners and nominated contact points) are appropriately informed of matters relating to individuals affected by the emergency.

Some changes to the proposed code were made as a result of submissions. The code, as finally issued, provided that in addition to applying while a state of emergency is in force, it would continue to apply for a further 20 working days to assist with recovery efforts.

The code was issued in March and commenced on 15 April. It applies automatically to any state of national emergency declared after that date.

Shortly after the end of the reporting year, the Office assisted the Ministry of Civil Defence and Emergency Management and the Auckland Council to hold a half day workshop on natural disasters and missing people.

Health Information Privacy Code

In March 2013, after a public submission process initiated in 2012, Amendment No.7 to the Health Information Privacy Code was issued.

The amendment to the code:

- created a regulatory regime for information derived from the new-born metabolic screening programme blood spot samples;
- allowed Medic Alert to use the National Health Index number as a unique identifier and health agencies to identify health practitioners by their common practitioner number;
- and amended the definition of 'serious threat' to harmonise it with sections 4 and 5 of the Privacy Amendment Act 2013.

Credit Reporting Privacy Code

Major changes to the Credit Reporting Privacy Code came into effect in April 2012. In particular, the changes permitted credit providers and credit reporters to move to a more comprehensive 'positive reporting' credit reporting system. Under

a positive system, credit reporters collect records of the actual amounts of credit extended to individuals. Lenders may then upload information on a monthly basis, showing whether or not individuals have met their monthly credit repayments. While the law was changed last year, the major changes anticipated in the consumer credit system will take some years to fully bed in. Positive reporting had not commenced by the end of the 2012/13 year.

In anticipation of positive reporting starting, the OPC undertook a series of public education initiatives. A series of educational materials built around seven 'key messages' were developed and used for a nationwide series of seminars for consumer advisers.

Seven key messages	
1.	Credit reporting helps credit providers decide whether to lend to you.
2.	Your borrowing reflects on you.
3.	Credit isn't just about borrowing money: power and phone companies also give credit.
4.	Regularly check your credit report, especially if you're about to seek credit.
5.	You have the right to seek correction of your credit information.
6.	If you believe you're at risk of identity fraud, ask credit reporters to 'freeze' your credit information until the risk has passed.
7.	There's more than one credit reporter: make sure you talk to them all.

During the year, two amendments were made to the credit reporting code:

- Amendment No. 7 made several changes, most notably permitting credit reporters to disclose credit information to credit providers and credit insurers for the purpose of identity verification under the Anti-Money Laundering and Countering Financing of Terrorism Act 2009.
- Amendment No. 8 changed the code's rules about the use and disclosure of credit information as it relates to serious threats. This aligned the code with changes made to the principles in the Privacy Act in a 2013 statutory amendment.

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 16 (previous year 22) consultations from the Ombudsman and completed and closed all 16.

As in previous years, the privacy interests that gave rise to the most consultations were those dealing with employment issues and job performance issues. Several related to access to information about criminal investigations.

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 protecting 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 or sharing 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 codes of practice and international issues.

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

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

The Public Affairs Manager is responsible for the communications and media work in the Office.

The Support Services Manager has responsibility for corporate services for the OPC.

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

Contract staff are variously involved in management, accounting and technical support work for the OPC.

Equal employment opportunities

The OPC promotes Equal Employment Opportunities (EEO) to ensure that its practices are in line with its obligations as a good employer. The Office has an EEO policy that is integrated with the human resource programmes outlined in the Statement of Intent 2013 and that encourages active staff participation in all EEO matters. These are reviewed annually.

During the 2012/13 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 Employment Opportunities Trust
- integrating 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 11: WORKPLACE GENDER PROFILE 2012/13

	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	4	1	1		6
Administrative support	5	2			7
Advisers (Technology & Policy)	1		2		3
Enquiries officers	1		1		2
Total	16	4	11		31

TABLE 12: WORKPLACE ETHNIC PROFILE 2012/13

	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		1		1				3	
Administrative support									5	2
Advisers (Technology & Policy)									3	
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 Privacy Commissioner's functions is to require government departments to report 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 Privacy Commissioner's reports are included in this chapter.

A detailed description of information matching and each active programme is on OPC's website at http://www.privacy.org.nz/information-sharing/information-sharing-introduction/.

Glossary

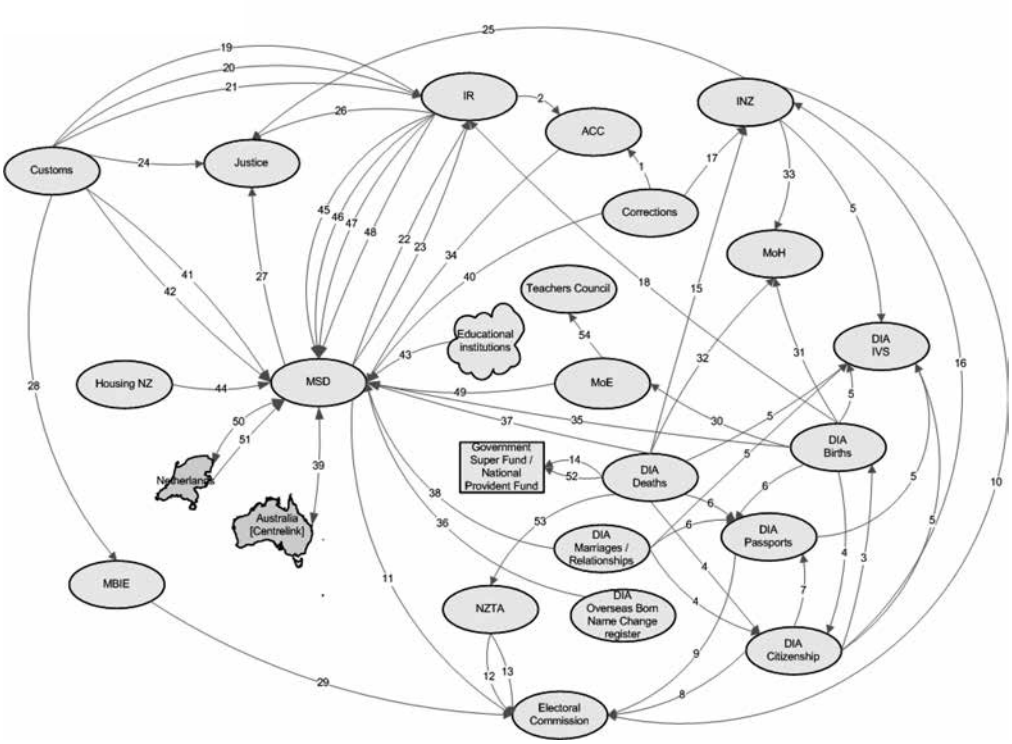
The following abbreviations and acronyms are used in this chapter:

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 MBIE)
IR	Inland Revenue
IVS	Identity Verification Service
Justice	Ministry of Justice
MBIE	Ministry of Business, Innovation and Employment
MoE	Ministry of Education
MoH	Ministry of Health
MSD	Ministry of Social Development
NHI	National Health Index
NPF	National Provident Fund
NSI	National Student Index
NZTA	New Zealand Transport Agency
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 54 active 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 4: ACTIVE AUTHORISED INFORMATION MATCHING PROGRAMMES 2012/13



Outreach

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

We ran one information matching and sharing workshop in March 2013 for nine staff from NZTA.

Changes in authorised and operating programmes

Parliament passed three information matching authorisations during the year.

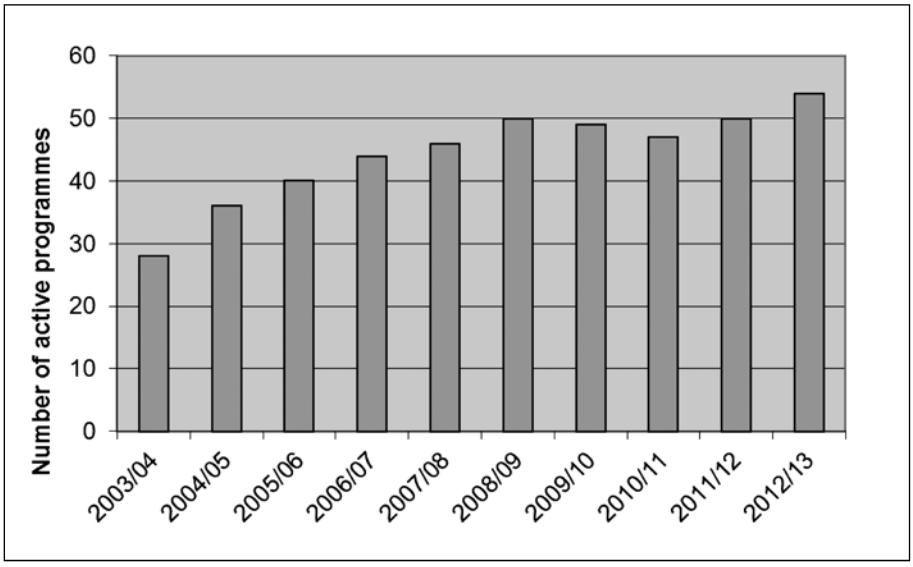
The Electronic Identity Verification Act 2012 was passed on 18 December 2012, authorising the now active programme that checks births, deaths, marriages, citizenship, passports and immigration information to support the igovt Identity Verification Service operated by DIA.

The Student Loan Scheme Amendment Act 2013 was passed on 29 March 2013, authorising the now active Customs/IR Student Loans Alerts programme.

The Social Security (Benefit Categories and Work Focus) Amendment Act 2013 was passed on 16 April 2013, authorising the Justice/MSD Warrants to Arrest Programme. This programme started in July 2013 and will be reported on next year.

- The following four new programmes went live during the year:
- BDM/MSD Overseas Born Name Change Programme
- BDM/IR Child Support Processing Programme
- DIA Identity Verification Service Programme (IVS)
- Customs/IR Student Loan Alerts Programme.

FIGURE 5: ACTIVE INFORMATION MATCHING PROGRAMMES 2004-2013



Periodic review (s.106) of information matching programmes

In September 2012, we reported to the Minister of Justice on a periodic review (s.106) of six information matching programmes (BDM(Deaths)/INZ Deceased Temporary Visa Holders; Citizenship/INZ Entitlement to Reside; Corrections/INZ Prisoners; Customs/Justice Fines Defaulters Alerts; INZ/Justice Fines Defaulters Tracing; IR/Justice Fines Defaulters Tracing). We recommended that these programmes continue. Our report is available at http://privacy.org.nz/information-sharing/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 have appropriate safeguards to protect the data.

The practice of OPC 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 2013, 41 of the 54 active programmes used online transfers. We approved 5 first-time approvals during 2012/13, and 16 renewals of existing approvals.

TABLE 13: FIRST TIME APPROVALS 2012/13

User agency Programme name (and number) Approval date	Reasons for granting	Grounds in support
DIA - Identity Verification Service (IVS)		
Identity verification (BDM) (programme 5) 9 April 2013	efficiency, transfer within agency	auditing enabled
Identity verification (Citizenship) (programme 5) 9 April 2013	efficiency, transfer within agency	auditing enabled
Identity verification (Passports) (programme 5) 9 April 2013	efficiency, transfer within agency	auditing enabled
Identity verification (Immigration) (programme 5) 9 April 2013	efficiency and security	auditing enabled
Inland Revenue		
New-borns tax number (active from 1 July 2013) 27 June 2013	efficiency and security	timely delivery of data.

TABLE 14: RENEWED APPROVALS 2012/13

User agency Programme name (and number) Approval date	Reasons for granting	Grounds in support
ACC		
Prisoners (programme 1) 3 July 2012	efficiency and security	satisfactory audit result
Prisoners (programme 1) 17 December 2012	efficiency and security	satisfactory audit result
Compensation and levies (programme 2) 5 April 2013	efficiency and security	timely delivery of data
Government Super Fund		
Eligibility (programme 14) 30 April 2013	efficiency and security	satisfactory audit result
Inland Revenue		
Working for families (programme 22) 8 April 2013	efficiency and security	satisfactory audit result
Child support alerts (programme 19) 16 August 2012	continued efficiency	satisfactory audit result
Child support alerts and student loan interest (programmes 19 and 21) 29 April 2013	continued efficiency	satisfactory audit result
Ministry of Business Innovation and Employment		
Motor vehicle traders importers (programme 28) 18 July 2012	efficiency and security	satisfactory audit result
Motor vehicle traders sellers (programme 29) 17 August 2013	efficiency and security	satisfactory audit result
Ministry of Health		
Publicly funded health eligibility (programme 33) 15 November 2012	efficiency and security	satisfactory audit result
Ministry of Justice		
Fines defaulters tracing (programme 27) 16 August 2012	efficiency and security	satisfactory audit result
Ministry of Social Development		
Benefit eligibility (programme 34) 10 October 2012	efficiency and security	satisfactory audit result
Commencement Cessation (programmes 45 and 46) 29 Oct 2012	efficiency and security	satisfactory audit result
Arrivals and departures (query access) (programme 41) 12 December 2012	efficiency and security	satisfactory audit result
National Provident Fund		
Eligibility (programme 52) 30 April 2013	efficiency and security	satisfactory audit result
New Zealand Transport Agency		
Deceased driver licence holders (programme 53) 10 October 2012	efficiency and security	satisfactory audit result

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 Part 10 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/information-sharing/operating-matching-programmes/.

How we assess programme compliance

Our assessment of a matching programme's compliance is based on the information provided to us by agencies as part of regular reporting, and any other issues drawn to our attention during the reporting period. Where agencies' reporting consists solely of statistical information, our compliance judgements are limited to what can be inferred from that information.

During 2012/13, we made changes to how we assess compliance in order to:

- streamline reporting requirements on agencies, and
- obtain evidence on compliance with each of the information matching rules.

In order to streamline reporting requirements, we reviewed the requirement for an annual audit to see whether it was still the most efficient way for us to get the information we need to manage privacy risks. We considered that requiring agencies to conduct an annual audit where there were no substantive issues identified in the previous year's audit report, and no substantive changes to the system used represented an unnecessary demand on agency resources. As a result we have changed our requirements so that an audit is required only at intervals of up to three years in these circumstances.

In lieu of an annual audit, we instead required a letter from the agency giving formal assurances about any changes made to the operation of the programme, measures taken to ensure people are aware of the match, measures taken to destroy information in accordance with the technical standards report, and the contents of adverse action letters sent as a result of the match. This change only affects the requirement for an audit and does not affect any requirements for statistics or other information that we normally receive about any of these programmes.

Through the review, we also identified that where programmes were not subject to regular audits, we did not have sufficient information to be fully confident about agencies' compliance with destruction requirements set out in Part 10 and Schedule 4 of the Privacy Act. This year, we have asked agencies to provided details about how they manage match information in order to comply with these requirements. This additional information has revealed that a number of matching programmes do not have sufficiently robust processes for destroying data in accordance with the Act. Where programmes have been found not to comply with destruction requirements, the specifics are set out in individual programme reports. We will be working with agencies to resolve these issues during the coming year.

We have also identified that where agencies are not carrying out regular audits, we do not have sufficient information to be completely confident that agencies always notify clients of an adverse action in accordance with s103 of the Privacy Act, and that agencies are taking sufficient steps to make individuals aware of a particular match. While these are not areas where we have particular concerns about agency compliance, we will be looking at opportunities to address these gaps ahead of next year's reporting.

This year we have also changed the way we describe programmes' compliance. There are three levels:

- **Compliant:** where the evidence we have been provided indicates that the programme complies with the information matching rules.
- **Not compliant – minor technical issues:** where reporting has identified practices that are not compliant with the information matching rules, but genuine efforts have been made to implement a compliant programme, and the risks to individual privacy are low.
- **Not compliant – substantive issues:** where reporting has identified practices that are not compliant with the information matching rules or other provisions of the Privacy Act that cannot be considered minor technical issues.

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.

2012/13 activity:

Match runs	49
Records received for matching	90,103
Possible matches identified	3,517
Overpayments established (number)	29
Overpayments established	$17,744
Average overpayment	$612
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 online weekly.

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.

2012/13 activity:

Self-employed people's records received for matching	546,636
Employers' records received for matching	527,999
Invoices issued to self-employed people	462,435
Invoices (individual employee) issued to employers	638,321
Challenges by individuals	38
Challenges by corporations	64
Total challenges	102
Successful challenges	8

Compliance: Compliant.

3 Citizenship/BDM Citizenship by Birth Processing Programme

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

Year commenced: 2006

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

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

2012/13 activity:

Births registered	61,633
Notices of adverse action	1, 495
Challenges received	269
Successful challenges	156
Citizenship by birth declined	1,393

Assurance has been received that operation of this programme has not changed and that no significant issues were identified during the year.

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.

2012/13 activity:

Applications for citizenship by descent (may include more than one person)	10,846
Notice of adverse action (arising from failure to match)	9
Successful challenges	2
Citizenship by descent registered	10,587

Assurance has been received that operation of this programme has not changed and that no significant issues were identified during the year.

Commentary: Notices of adverse action are sent when citizenship staff 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 DIA Identity Verification Service Programme (IVS)

Purpose: To verify identity information provided by an applicant in support of their application for the issue, renewal, amendment, or cancellation of an electronic identity credential (EIC), or to keep the core information contained in an EIC accurate and up to date.

Year commenced: 2013

Features: Data is transferred online when each application is processed.

Disclosures:

- Births disclosure to IVS: Child's names, gender, birth date and birth place and country, citizenship by birth status, marriage date, registration number, mother's names, father's names, since died indicator and stillborn indicator.
- Deaths disclosure to IVS: Names, gender, date of birth, place of birth, date of death, place of death and age at death.
- Marriages disclosure to IVS: Names, date of birth, date of marriage, registration number, country of birth, gender, place of marriage, spouse's names.
- Citizenship disclosure to IVS: Names, gender, birth date, birth place, photograph, citizenship person identifier, citizenship certificate number, certificate type and certificate status.
- Passports disclosure to IVS: Names, gender, date of birth, place of birth, photograph, passport person identifier, passport number, date passport issued, date passport expired and passport status.
- Immigration disclosure to IVS: Whether a match is found, client ID number and any of the pre-defined set of identity related alerts.

2012/13 activity:

EIC applications	805
EIC applications abandoned	421
EICs issued	227

EICs cancelled	0
Number of challenges to discrepancies	0
Sent to INZ for matching	50
Not issued based on INZ match	0
Number of Agencies allowing access using EICs	1
Number of times EICs have been used	132

Commentary: Matches to Births, Deaths, Marriages Citizenship and Passports are all looked up by the IVS system when an IVS application is processed. Applicant details are only sent to INZ when the application is based on immigration documents (to verify the application) or the applicant may hold immigration documents (to ensure the application is not a duplicate).

Compliance: Compliant.

6 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.

2012/13 activity:

Passport applications	632,906
Possible matches: Births	1,777,189
Possible matches: Marriage/Relationships	91,904
Possible matches: Deaths	3,257,715
Notice of adverse action	5,310
Successful challenges	5,070
Passports issued (diplomatic, official and standard)	615,584

We have been assured that operation of this programme has not changed and that no significant issues were identified during the year.

Commentary: Notices of adverse action are sent when passports staff 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.

7 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.

2012/13 activity:

Passport applications	632,906
Possible matches to Citizenship records	488,459
Notice of adverse action	855
Successful challenges	815
Passports issued (diplomatic, official and standard)	615,584

We have been assured that operation of this programme has not changed and that no significant issues were identified during the year.

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.

8 Citizenship/EC 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 EC: Citizenship provides full name, date of birth and residential address of new citizens aged 17 years and over (by grant or by descent).

2012/13 activity:

Match runs	4
Records received for matching	23,041
Invitations to enrol sent out	863
Presumed delivered	844
New enrolments	100
Percentage of letters delivered resulting in changes	12%
No response	744
Cost	$798
Average cost per enrolment	$7.98

Compliance: Compliant.

9 DIA (Passports)/EC 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 EC: Passports provides full name, date of birth and residential address of passport holders aged 17 years and over

2012/13 activity:

Match runs	4
Records received for matching	372,194
Invitations to enrol sent out	21,251
Presumed delivered	20,477
New and updated enrolments	3,135
Percentage of letters delivered resulting in changes	15%
No response	17,342
Cost	$15,442
Average cost per enrolment	$4.93

Compliance: Compliant.

10 INZ/EC 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 EC: 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.

2012/13 activity:

Records received for matching (on 30 June 2013)	215,881
Possible matches identified	728
Notice of adverse action sent[2]	728
Challenges received	17
Successful challenges	16
Cost	$3,030.45

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

Compliance: Compliant.

11 MSD/EC 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 EC: 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.

2012/13 activity:

Match runs	4
Records received for matching	640,591

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

Invitations to enrol sent out	138,485
Presumed delivered	134,700
New and updated enrolments	21,170
Percentage of letters delivered resulting in changes	16%
No response	113,530
Cost	$100,102
Average cost per enrolment	$4.73

Compliance: Compliant.

12 NZTA (Driver Licence)/EC 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 EC: 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.

2012/13 activity:

Match runs	4
Records received for matching	934,276
Invitations to enrol sent out	158,923
Invitations presumed delivered	153,195
New and updated enrolments	28,915
Percentage of letters delivered resulting in changes	19%
No response	124,280
Cost	$116,894.39
Average cost per enrolment	$4.04

Compliance: Compliant.

13 NZTA (Vehicle Registration)/EC 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.

NZTA disclosure to EC:NZTA 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.

2012/13 activity:

Match runs	4
Records received for matching	1,232,251
Invitations to enrol sent out	157,908
Invitations presumed delivered	151,928
New and updated enrolments	26,060
Percentage of letters delivered resulting in changes	17%
No response	125,868
Cost	$115,076
Average cost per enrolment	$4.42

Compliance: Compliant.

14 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).

2012/13 activity:

Records received for matching	30,235
Possible matches identified	9,486
Notices of adverse action sent	678
Challenges	0

Compliance: Compliant.

15 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.

2012/13 activity:

Match runs	2
Records received for matching	29,129
Possible matches identified	849
Records marked as deceased - overstayer list	117
Records marked as deceased - temporary visa holders' list	47
Total number of records updated as deceased	164

Compliance: Compliant.

16 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.

2012/13 activity:

Match runs	3
Records received for matching	1,279,143
Possible matches identified	6,886
Number of NZ citizens removed from the overstayer list	435

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.

Compliance: Compliant.

17 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.

2012/13 Activity:

Match runs	52
Possible matches identified	378
Cases excluded as not being eligible for removal or deportation	333
Notices of adverse action	45
Successful challenges	1
Cases considered for removal and deportation	43
Removals and deportations from NZ at year's end	27

Commentary: From August 2013, individuals sentenced to home detention are included in this programme and will be reported on next year.

Compliance: Not compliant - minor technical issues.

As part of a review of how we assess each programme, we found that information received from Corrections is not fully destroyed, in accordance with section 101 of the Act. While data is removed from view, the data still resides within Immigration's database for a longer period. Because the data is not available to be acted on without significant additional effort on the part of Immigration, we consider the risk of harm to individuals is low, and that this is a minor technical issue. We will be working with INZ to resolve this issue during the coming year.

18 BDM (Births)/IR Child Support Processing Programme

Purpose: To allocate IRD numbers to individuals within the child support scheme, in particular qualifying and dependent children by confirming their birth details.

Year commenced: 2013 (January)

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

BDM disclosure to IR: BDM provides birth information covering the period from 1 April 1994 to the extraction date. The birth details include the full name, date and place of birth, birth registration number and full name and date of birth of both mother and father.

2012/13 Activity:

Children without IR number for child support (as at January 2013)	27,658
Children with tax number already allocated by IR but not assigned in child support records	3,718
Birth record confirmed for existing child in child support scheme (IR number allocated)	20,271
Child birth record not found (likely born overseas)	3,485
Birth record confirmed for new child in child support scheme (IR number allocated)	2,884

Commentary: This programme enables Inland Revenue to allocate an IR number to a child by confirming identity details held by Inland Revenue or in a child support application against the details held in the birth registration extract provided by DIA. Where birth information is not matched, Inland Revenue requires that the customer provide details of identity, such as an overseas birth certificate.

Compliance: Not compliant - substantive issues.

During Inland Revenue's audit of this programme it found that steps had not been taken to inform the public about the existence of the programme as required under the information matching rules. Inland Revenue has now updated its website with information.

19 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).

2012/13 Activity:

Possible matches identified	10,060
Arrival cards received for liable parents	1,057
Cards not useable or did not meet matching criteria	96
Remaining cards where contact attempted with liable parent	961
New contact details updated	212
Existing contact details confirmed	379
Contact details not useful	370

Commentary: Despite a 42% increase in possible matches identified (7,108 in 2011/12), the number of contacts with liable parents is similar to last year.

An audit of the operation of this programme in 2011/12 found that there are effective controls in place. We received a letter of assurance that noted changes in this programme to include overseas based student loan borrowers in serious default. However the changes did not require any amendment to the technical standards report governing the programme. Details about student loan borrowers are reported separately under the Customs/IR Student Loan Alerts Programme.

In the absence of any changes to the operation of the programme, the next audit will be required in 2014/15.

Compliance: Compliant.

20 Customs/IR Student Loan Alerts Programme

Purpose: To identify overseas based borrowers in serious default of their student loan repayment obligations who leave for or return from overseas so that IR can take steps to recover the outstanding debt.

Year commenced: 2013

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 borrowers in serious default of their student loan obligations.

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).

2012/13 Activity:

This programme commenced operating on 30 April 2013. We agreed with Inland Revenue that reporting on activity for this programme will start next year.

Commentary: This programme has not been fully assessed for compliance but will be included in Inland Revenue's audit programme this coming year. No significant issues have occurred in its first two months of operation..

Compliance: Not assessed.

21 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.

2012/13 Activity: There were 543,019 borrower records (485,464 last year) updated as a result of matching student borrower records with travel movement information held by Customs. This year's figure is for the 1 July to 30 June period, reporting in previous years was for the tax year (1 April – 31 March).

Commentary: An audit of the operation of this programme in 2011/12 found that there are effective controls in place. We received a letter of assurance that noted no changes have been made to the operation of the programme and no difficulties have been experienced. In the absence of any changes to the operation of the programme, the next audit will be in 2014/15.

Compliance: Compliant.

22 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.

2012/13 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 of the operation of this programme in 2011/12 found that there are effective controls in place. We received a letter of assurance that noted no changes have been made to the operation of the programme and no difficulties have been experienced. In the absence of any changes to the operation of the programme, the next audit will be in 2014/15.

Compliance: Compliant.

23 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.

2012/13 Activity: Inland Revenue estimates annual savings of $3.0 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 approximately 970 and $300,000 respectively. Exact figures for the full year are not available due to an IR process error (now rectified).

Commentary: An audit of the operation of this programme in 2011/12 found that there are effective controls in place but noted that work to refresh the information matching agreement has been delayed.

This year, IR reports that the agreement will be updated after changes affecting tax credit calculations are passed as part of the Taxation (Annual Rates, Foreign Superannuation, and Remedial Matters) Bill currently before Parliament.

In the absence of any changes to the operation of the programme, the next audit will be in 2014/15.

Compliance: Compliant.

24 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.

2012/13 Activity:

Silent alerts triggered	6,167
Individuals subject to silent alerts	2,916
Intercept alerts triggered	201
People intercepted[7]	171
On departure	59
On arrival	135
Incorrect intercepts	6
Fines had already been paid	6
Wrong person identified by the match	0
Interception not completed	17
Fines received	$47,990
Reparation received	$81,435
Amount under a current time to pay arrangement	$215,567
Remittals/ Alternative sentence imposed	$140,682

Commentary: As at 30 June, there were 3,886 fines defaulters who had interception alerts recorded against their names in Customs records, up from 3,701 last year. There were also 21,609 fines defaulters who had silent alerts recorded, up from 21,267 last year.

Compliance: Not compliant - minor technical issues.

On two occasions during the year fines defaulter information was not updated onto the Customs alerts system. As a result, one individual was intercepted at the airport despite having paid their fines a day earlier. Justice is working with Customs to implement a permanent solution to fix the fault. In the meantime manual steps are being taken to prevent a recurrence.

25 INZ/Justice Fines Defaulters Tracing Programme

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

Year commenced: 2006

Features: Data transferred weekly by online transfer.

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

INZ disclosure to Justice: INZ supplies information contained on the arrival and

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

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).

2012/13 Activity:

Records sent to INZ	5,285
Notices of adverse action	356
Successful challenges	0
Payment received for fines	$70,759
Amounts under a current time-to-pay arrangement	$86,406
Remittals/alternative sentence imposed	$106,648

Commentary: The effectiveness of this programme appears to be waning with payments, amounts under time-to-pay arrangement and remittals at their lowest levels since this programme commenced. Justice is finding that address details obtained from arrival and departure cards are often a repeat of information already held and known to be invalid.

Compliance: Not compliant - substantive issues.

As part of a review into how we assess each programme, we identified that Justice was not destroying information received from Immigration in accordance with the conditions in the information matching agreement. Justice has taken steps to fix this issue.

26 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 daily using encrypted USB stick.

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

IR disclosure to Justice: For matched records, IR supplies 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.

2012/13 Activity:

Processing Activity

	July to December 2012	January to June 2013
	Final figures	Progress figures
Match runs	114	116
Records sent for matching	1,014,925	1,169,932
Possible matches identified	405,038	459,730
Notices of adverse action	139,507	134,365
Challenges	650	637
Successful challenges	56	31

Financial Outcome Activity

		July to December 2012	January to June 2013
		Final figures	Progress figures
Paid/settled ($)	IR	17,310,098	27,515,359
	MSD	13,104,688	16,300,242
	Both	12,875,759	14,390,787
Total paid/settled ($)		43,290,545	58,206,389
People with payment or remittal	IR	33,042	70,849
	MSD	22,105	42,551
	Both	24,388	40,700
Total people with payment or remittal		79,535	154,100

Commentary: Results for the first six months of 2013 show that nearly twice the number of people paid or had their fines remitted compared to the previous six months. Also significant is the increase in the value of payments received or remitted for this programme compared to the sibling MSD programme. Justice reports that it cannot attribute the increase to a specific business initiative.

Compliance: Not compliant - substantive issues.

As part of a review into how we assess each programme, we identified that Justice is not destroying information received from Inland Revenue in accordance with the conditions contained in the information matching agreement. We will be working with Justice to resolve this issue during the coming year.

27 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 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 a data matching reference number to MSD.

MSD disclosure to Justice: For matched records, MSD returns the last known residential address, postal address, residential, cell-phone and work phone numbers, and the unique identifier originally provided by Justice.

2012/13 Activity:

Processing Activity

	July to December 2012	January to June 2013
	Final figures	Progress figures
Match runs	116	117
Records sent for matching	1,000,604	1,130,289
Possible matches identified	265,100	303,599
Notices of adverse action	88,965	82,297
Challenges	380	443
Successful challenges	34	29

Financial Outcome Activity

		July to December 2012	January to June 2013
		Final figures	Progress figures
Paid/settled ($)	IR	17,310,098	27,515,359
	MSD	13,104,688	16,300,242
	Both	12,875,759	14,390,787
Total paid/settled ($)		43,290,545	58,206,389
People with payment or remittal	IR	33,042	70,849
	MSD	22,105	42,551
	Both	24,388	40,700
Total people with payment or remittal		79,535	154,100

Commentary: Results for the first six months of 2013 show that nearly twice the number of people paid or had their fines remitted compared to the previous six months. Justice reports that it cannot attribute the increase to a specific business initiative.

Compliance: Not compliant - substantive issues.

As part of a review of how we assess each programme, we identified that Justice is not destroying information received from Inland Revenue in accordance with the conditions in the information matching agreement. We will be working with Justice to resolve this issue during the coming year.

28 Customs/MBIE Motor Vehicle Traders Importers Programme

Purpose: 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 MBIE: Customs provides MBIE 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.

2012/13 Activity:

Match runs		12
Records received for matching		3,964
Individuals or entities of interest identified		286
Notices of adverse action sent		415
Successful challenges	Entities: registered under another name	7
	Entities: primary purpose not financial gain	57
Entities referred to the National Enforcement Unit		9
Registrations as a result of notices of adverse action		28
No response to letters		33

Commentary: This is the first time that MBIE has completed a full year of matching. Previously, competing resource issues impeded its ability to consistently operate the programme.

Compliance: Not compliant - substantive issues.

As part of a review of how we assess each programme, we found that in some instances information received from Customs is not being destroyed in a sufficiently timely manner to comply with section 101 of the Act. MBIE has committed to review and modify its current processes so that it complies with the destruction requirements.

29 NZTA/ MBIE Motor Vehicle Traders Sellers Programme

Purpose: 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.

NZTA disclosure to MBIE: NZTA provides MBIE 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.

MBIE disclosure to MoT: MBIE provides NZTA 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.

2012/13 Activity:

Match runs		11
Records received for matching		27,837
Individuals or entities of interest identified		585
Notices of adverse action sent		980
Successful challenges	Entities: registered under another name	14
	Entities: primary purpose not financial gain	104
Entities referred to the National Enforcement Unit		167
Registrations as a result of notices of adverse action		54
No response to letters		191

Commentary: MBIE report that the majority of unregistered traders contacted have ceased their selling activity rather than register as motor vehicle traders.

Compliance: Not compliant - substantive issues.

As part of a review of how we assess each programme, we found that in some instances information received from NZTA is not being destroyed in a sufficiently timely manner to comply with section 101 of the Act. MBIE has committed to review and modify its current processes so that it complies with the destruction requirements.

30 BDM (Births)/MoE Student Birth Confirmation Programme

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

Year commenced: 2004

Features: Data is transferred on request on CD.

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

2012/13 activity:

Birth records from the period:	01 Jan 2005 - 30 Jun 2007	05 Sep 08 - 31 Jan 2013
Received for matching	152,194	276,580
Matched exactly with NSI record (automatically)	109,189	22,846
Matched after manual intervention	1,056	0

Total birth records matched	110,509	22,846
Total birth records not matched	41,685	0
Percentage matched	72.6%	8.3%

Birth records for the period 1 July 2007 to 1 September 2008 have been received but have not yet been matched.

Compliance: Compliant.

31 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.

2012/13 activity:

Records received for matching	61,220
Possible matches identified	61,220
Records not matched	0

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

Compliance: Compliant.

32 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.

2012/13 activity:

Records received for matching	30,141
Possible matches identified	26,758

Records manually matched	3,281
New NHIs allocated	102
Corrections to matches (including from previous years matches)	14

Compliance: Not compliant - substantive issues.

After completing the authorised matching, MoH retains the full data received for a year to help match coroner's reports to the mortality register when needed.

This is a breach of the time limits specified in the Privacy Act 1993 and 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. This issue has been raised in previous reports and has been repeatedly raised with MoH.

MoH does not issue adverse action notices in accordance with section 103 of the Privacy Act. MoH makes the NHI available to other agencies such as DHBs which may then rely on the information, even though the recorded deaths have not been verified. MoH has not been directly verifying the death matching as MoH has no direct interaction with the individuals. MoH does try to minimise the risk as far as practicable. It attempts to verify deaths by matching against other datasets it holds that deaths are reported in.

MoH makes NHI information available in two ways:

- MoH provides files to health providers for updating their records. MoH has added a warning to these files that the death information has not been verified.
- MoH makes the NHI accessible online to authorised users. MoH has changed this system to indicate the source of the death information. This new information will be available to users when they update their systems that allow them to access the NHI.

We do not know how effective these measures will be in reducing the risk to individuals who are incorrectly notified as deceased on the NHI.

33 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, if requested.

2012/13 activity:

Records sent for matching		470,349
Records matched		329,888
Notices of adverse action		9,115
Successful challenges	(wrongly matched)	2
	(error in application of eligibility criteria)	187

Compliance: Compliant.

34 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.

2012/13 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	1,712,358
Possible matches identified	5,195
All processing activity during the reporting period	
Matches that required no further action	3,401
Notices of adverse action	1,840
Challenges	105
Successful challenges	63
Overpayments established	1,354
Value of overpayments established	$1,377,807
Arrears paid	115
Value of arrears paid	$41,840

MSD receives address details through this programme to enable it to re-establish contact with former (non-current) clients who have outstanding benefit debts and to arrange repayment.

Debt recovery notification results

Notifications received	412
Notices of adverse action	83
Challenges	0
Debtors under arrangement to pay	8
Balance owed under arrangement	$4,999
Debtors paid in full	$6,290
Total recovered	$16,471

Commentary: MSD has refined the data matching criteria for debt recovery notifications resulting in fewer, but higher quality match results. The amount under arrangement has dropped significantly ($182,855 in 2012) and total recoveries is lower also ($16,471 last year).

Compliance: Not Compliant - substantive and minor technical issues.

As part of a review of how we assess each programme, we identified two areas of non compliance; one specific to this programme, and one common to all programmes operated at MSD's Integrity Intervention Centre.

Substantive issues:

We found that this programme uses the IRD number in a manner that breaches principle 12(2) of the Act. An agency cannot assign a unique identifier to an individual if it has been assigned to that individual by another agency. In our view, that includes situations where two agencies are using a third agency's unique identifier to assist matching of records.

While this programme has operated in this way for some time, it was not an issue that we had identified before. We advised MSD of this issue in December, and in February MSD made changes to prevent use of the IRD number by staff at the centre. MSD is doing further work to remove the IRD number from the ACC extract and update the technical standards report governing this programme.

Minor technical issues:

For all the programmes operated at the centre, we found that information received from other agencies is not fully destroyed in accordance with section 101 of the Act. While data is removed from view in a timely manner so that it cannot be acted upon, the data resides within MSD's database for up to 2.5 years before a purging process is completed.

Because the data is not available to be acted on without significant additional effort on the part of MSD, we consider the risk of harm to individuals is low, and that this is a minor technical issue. MSD has scheduled a review in the coming reporting period to address this issue.

35 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.

2012/13 Activity:

Benefit applications processed	298,382
Possible matches identified	13,278
All processing activity in the reporting period	
Matches that required no further action	966
Action taken with no overpayment	12,804
Notices of possible adverse action	23
Challenges	0
Overpayments established	0

Commentary: This programme often identifies minor errors within the client record that are corrected, but the changes do not result in overpayments.

Compliance: Not compliant- minor technical issues (refer to programme 34 commentary).

36 BDM/MSD Overseas Born Name Change Programme

Purpose: To verify a client's eligibility or continuing eligibility to a benefit where a client has legally changed their name in New Zealand and not informed MSD. The programme is also used to identify debtors and suspected benefit fraud.

Year commenced: 2012

Features: Data is transferred quarterly by encrypted CD.

BDM disclosure to MSD: BDM provides name change records from January 2009 to the extract date. The name change details include the full name at birth, former full name, new full name, birth date, residential address, and country of birth.

2012/13 Activity:

Match runs	4
Records received for matching	25,104
Possible matches identified	762
Matches that required no further action	152
Notices of adverse action	618
Challenges	2
Successful challenges	2
Overpayments established	8
Value of overpayments established	$245,802

Commentary: This programme started operating in November 2012. Of the overpayments established, the largest single overpayment was $130,549. The programme allows aliases to be added to client records and identifies clients receiving payments under more than one identity.

Compliance: Not compliant - minor technical issues (refer to programme 34 commentary).

37 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.

2012/13 Activity:

New match runs started in the reporting period	
Match runs	52
Records received for matching	30,326
Possible matches identified	6,000
All processing activity in the reporting period	
Matches that required no further action	3,270
Notices of adverse action	2,737
Challenges	0
Overpayments established	299
Value of overpayments established	$130,068

Compliance: Not compliant - minor technical issues (refer to programme 34 commentary).

38 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.

2012/13 Activity:

New match runs started in the reporting period	
Match runs	52
Records received for matching	22,595
Possible matches identified	2,570
All processing activity in the reporting period	
Matches that required no further action	1,288
Notices of adverse action	1,297
Successful challenges	5
Overpayments established	431
Value of overpayments established	$382,733

Compliance: Not compliant - minor technical issues (refer to programme 34 commentary).

39 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.

2012/13 activity:

Changes of information received by MSD from Centrelink	701,575
Notices of adverse action	7,558
Changes of information sent by MSD to Centrelink	259,643

Compliance: Compliant.

40 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.

2012/13 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	357
Records received for matching	17,043,622
Possible matches identified	13,210
All processing activity in the reporting period	
Matches that required no further action	4,380
Notices of adverse action	8,910
Challenges	8
Successful challenges	7
Overpayments established	1,980
Value of overpayments established	$212,469

MSD receives address details through this programme to enable it to re-establish contact with former (non-current) clients who have outstanding benefit debt and arrange repayment. MSD has refined the data matching criteria for debt recovery notifications resulting in fewer, but higher quality, match results.

Debt recovery notification results

Notifications received	1,240
Notices of adverse action	478
Challenges	0
Debtors under arrangement to pay	7
Balance owed under arrangement	$6,471
Total recovered	$2,994

Compliance: Not compliant - minor technical issues (refer to programme 34 commentary).

41 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.

2012/13 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	10,135,233
Possible matches identified	47,926
All processing activity in the reporting period	
Matches that required no further action	16,709
Notices of adverse action	32,679
Successful challenges	146
Overpayments established	23,103
Value of overpayments established	$13,363,129
Arrears paid	1
Value of arrears paid	$377

MSD receives address details through this programme to enable it to re-establish contact with former (non-current) clients who have outstanding benefit debts and to arrange repayment.

Debt recovery notification results

Notifications received	1,516
Notices of adverse action	755
Challenges	0
Debtors under arrangement to pay	40
Balance owed under arrangement	$354,187
Total recovered	$50,202

Commentary: MSD has refined the debt recovery notifications matching algorithm to provide for lower volume but higher quality match results (84,696 notifications last year). However, the total recovered has dropped by about 50%.

Compliance: Not compliant - minor technical issues (refer to programme 34 commentary).

42 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.

2012/13 activity: MSD staff accessed 127 Customs records.

Compliance: Not compliant - minor technical issues.

An audit on the operation of this programme found printouts were not being destroyed within a month of printing because the quality assurance review was scheduled to be done monthly and the printouts were retained until the review was completed. These reviews are now done fortnightly.

43 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.

2012/13 activity:

Educational institutions involved in the matching programme	612
Records sent for matching	883,293
Individual applicants involved in matching	214,690
Notices of adverse action sent out (individuals may receive more than one)	38,636
Challenges	123
Successful challenges	36
Decisions to decline loan/allowance	21,881

Compliance: Compliant.

44 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. Details about the property location, tenancy start / end dates, weekly rental charges and any forwarding address provided on termination of the tenancy are also included.

2012/13 Activity:

New match runs started in the reporting period	
Match runs	50
Records received for matching	97,317
Possible matches identified	16,562
All processing activity in the reporting period	
Matches that required no further action	16,263
Notices of adverse action	304
Challenges	5
Overpayments established	11
Value of overpayments established	$6,095

Commentary: Our recently completed section 106 review of this programme recommended that MSD either cease operating this programme and divert resources into other programmes, or modify the operation of the programme to improve its return on investment.

A change to HNZ systems in August 2012 has meant MSD is receiving more possible matches through this programme. While there was a six-fold increase in the number of notices of adverse action sent, the discrepancies uncovered have not resulted in an increase in overpayments being established.

MSD is to review the programme as part of changes in its responsibilities relating to social housing in April 2014.

Compliance: Not compliant - minor technical issues (refer to programme 34 commentary).

45 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.

2012/13 Activity:

New match runs started in the reporting period	
Match runs	12
Records sent for matching	27,663
Possible matches identified	1,203
All processing activity in the reporting period	
Matches that required no further action	499
Notices of adverse action	606
Challenges	23
Successful challenges	15
Overpayments established	2,192
Value of overpayments established	$18,880,590
Arrears paid	13
Value of arrears paid	$13,238

Commentary: MSD sent a limited number of records to Inland Revenue this year. The reduction in records sent was in anticipation of a change-over to new information sharing processes under section 81BA of the Tax Administration Act that commenced in March 2013.

Compliance: Not compliant - minor technical issues (refer to programme 34 commentary).

46 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.

2012/13 Activity:

New match runs started in the reporting period	
Match runs	8
Records sent for matching	7,588
Possible matches identified	3,330
All match runs active in the reporting period	
Matches that required no further action	2,016
Notices of adverse action	1,319
Challenges	35
Successful challenges	28
Overpayments established	338
Value of overpayments established	$441,128

Commentary: MSD sent a limited number of records to Inland Revenue this year. The reduction in records sent was in anticipation of a change-over to new information sharing processes under section 81BA of the Tax Administration Act that commenced in March 2013.

Compliance: Not compliant - minor technical issues (refer to programme 34 commentary).

47 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.

2012/13 activity:

Match runs	50
Records received for matching	1,585,655
CSCs automatically renewed	171,541
'Invitation to Apply' forms sent out	85,899
Notices of adverse action	20,577
Challenges	59
Successful challenges	59
Unsuccessful challenges	12

Commentary: Last year, MSD advised that income definitions for the CSC were not aligned with IR statutory definitions of family credit income. MSD now advises that IR will include the necessary amendments to the definitions in a bill in 2013. Cards have been issued to an estimated 1,100 people who may not qualify if income was correctly assessed.

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

48 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.

2012/13 activity: No requests for information were received from the Netherlands.

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

Compliance: Compliant.

49 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.

2012/13 activity:

Allowance applications

Records sent for matching (including repeat requests)	103,062
Individual applications involved in matching	71,342
Notices of adverse action	5,613
Successful challenges[8]	2,257

Loan applications

Records sent for matching	14,639
Notices of adverse action	1,164
Successful challenges	181

Commentary: Challenges to adverse action notices are usually resolved by the applicant providing clarification or updated information when contacted. "Successful challenges" include those 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.

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 a letter subsequently 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: Not compliant - substantive issue

MSD provides an applicant's IRD number (where known) to MoE to use in the matching process. The use of IRD numbers is contrary to privacy principle 12(2) of the Privacy Act 1993, which prevents an agency from assigning another agency's unique identifier.

This issue was not identified by MSD or OPC when the match was set up in 2006, probably because the match made use of an existing system. MoE had

set up this system in 2001 to receive and hold IRD numbers to facilitate the processing of student loan interest write-offs. The student loan interest write-offs ceased in 2007. This is expected to be replaced when the proposed tertiary education information reporting project is implemented. OPC has requested MSD ask MoE what cost, if any, there might be in changing the existing matching algorithm.

50 Netherlands/MSD Change in Circumstances Programme

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

Year commenced: 2003

Features: Manual transfer of completed application forms as required.

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

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

2012/13 activity: As an indicator of activity, MSD issued 411 notices of adverse action. This figure includes some corrections to SVB reference numbers. There were no challenges to these notices.

Compliance: Compliant.

51 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.

2021/13 activity: MSD made deductions from pension payments to 3,727 people. There were 1,278 MSD clients resident in the Netherlands.

Compliance: Compliant.

52 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 online.

BDM disclosure to NPF: BDM provides information from the deaths register for 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).

2012/13 activity:

Records received for matching	35,125
Possible matches identified - Pensioners	398
Possible matches identified - Contributors	167
Notices of adverse action sent	565
Challenges	0

Compliance: Compliant.

53 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.

2012/13 Activity:

Match runs	26
Records received for matching	30,256
Possible matches identified	19,846
Notices of adverse action	12,048
Challenges	1
Successful challenges	1
Courtesy letters sent	5,883
Driver licence records cancelled	18,489

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: Not compliant - substantive issues.

As part of a review of how we assess each programme, we asked NZTA to explain how they complied with the destruction rules in the Act. NZTA found that it was not deleting the death information once it had been used, so was not complying with section 101(4) of the Act.

NZTA has since confirmed it has deleted the retained death information; that no other action other than the original action has been taken using the data, and its ongoing business practices have been modified.

54 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).

2012/13 Teachers Council activity:

Match runs	13
Average number records received from MoE in a match run	56,625
Matched, letter sent to establish registration status	4,804
Successful challenges	53
Not matched, letter sent	315
Match resolved by teacher response	217
Issues in process of being resolved	155
Number of matches confirmed by contact (cumulative)	4,232

Commentary: There was no action based on the match by MoE in this year.

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 2013.

Privacy Commissioner
M Shroff
30 October 2013

General Manager
G F Bulog
30 October 2013

AUDIT NEW ZEALAND
Mana Arotake Aotearoa

Independent Auditor's Report

To the readers of Office of the Privacy Commissioner's financial statements and non-financial performance information for the year ended 30 June 2013

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

We have audited:

- the financial statements of the Privacy Commissioner on pages 111 to 136, that comprise the statement of financial position as at 30 June 2013, 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 non-financial performance information of the Privacy Commissioner on pages 101 to 110, that comprises the statement of service performance and which includes outcomes.

Opinion

In our opinion:

- the financial statements of the Privacy Commissioner on pages 111 to 136:
  - comply with generally accepted accounting practice in New Zealand; and
  - fairly reflect the Privacy Commissioner's:
    - financial position as at 30 June 2013; and
    - financial performance and cash flows for the year ended on that date.
- the non-financial performance information of the Privacy Commissioner on pages 101 to 110:
  - complies with generally accepted accounting practice in New Zealand; and
  - fairly reflects the Privacy Commissioner's service performance for the year ended 30 June 2013, including for each class of outputs:
    - its service performance compared with forecasts in the statement of forecast service performance at the start of the financial year; and

- its 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 30 October 2013. 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 non-financial performance information are free from material misstatement.

Material misstatements are differences or omissions of amounts and disclosures that, in our judgement, are likely to influence readers' overall understanding of the financial statements and non-financial performance information. 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 non-financial performance information. The procedures selected depend on our judgement, including our assessment of risks of material misstatement of the financial statements and non-financial performance information, 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 non-financial performance information 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 appropriateness of the reported non-financial performance information within the Privacy Commissioner's framework for reporting performance;
- the adequacy of all disclosures in the financial statements and non-financial performance information; and
- the overall presentation of the financial statements and non-financial performance information.

We did not examine every transaction, nor do we guarantee complete accuracy of the financial statements and non-financial performance information. Also we did not evaluate the

security and controls over the electronic publication of the financial statements and non-financial performance information.

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 non-financial performance information 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 and outcomes.

The Privacy Commissioner is also responsible for such internal control as is determined necessary to enable the preparation of financial statements and non-financial performance information that are free from material misstatement, whether due to fraud or error. The Privacy Commissioner is also responsible for the publication of the financial statements and non-financial performance information, whether in printed or electronic form.

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 non-financial performance information 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 External Reporting Board.

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

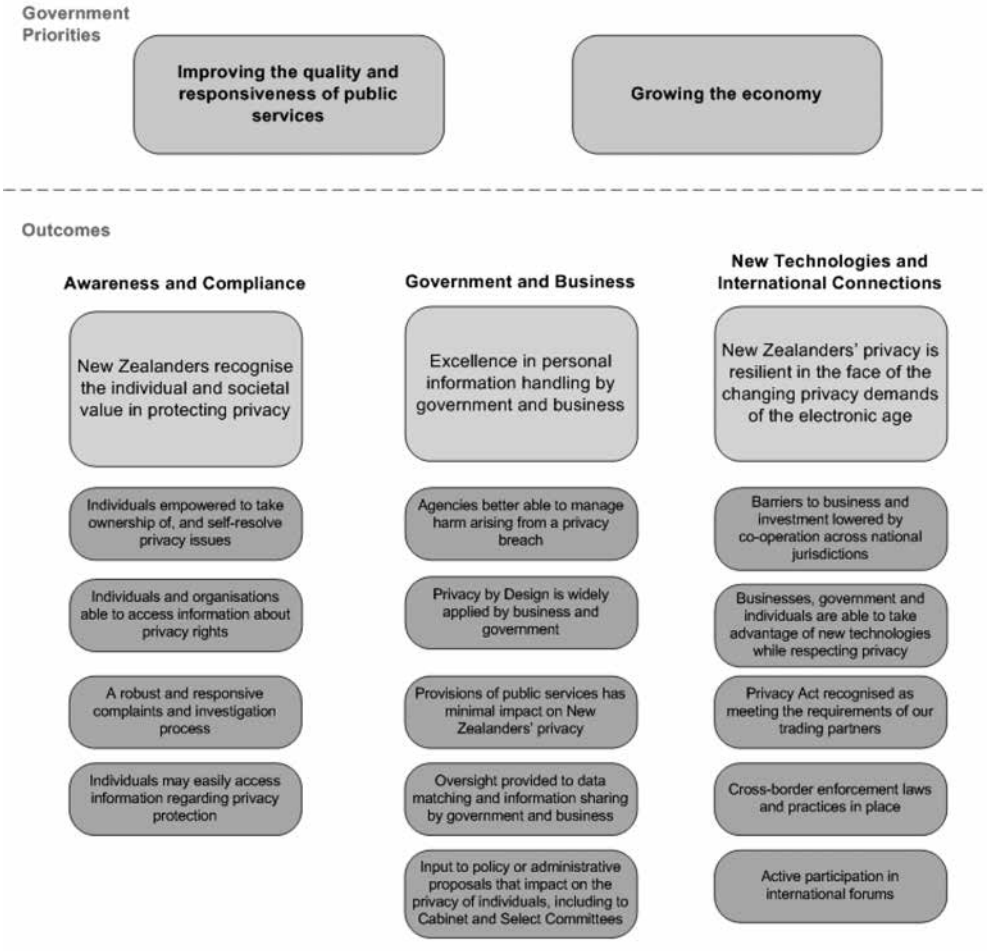
STATEMENT OF OBJECTIVES AND SERVICE PERFORMANCE 2012/13

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 and responsiveness of public services.

A set of performance measures has been developed to provide a means to demonstrate both internally and externally that the Office is performing effectively in achieving the stated outcomes.

The Office works towards three long term outcomes through the targeted and flexible use of its resources. The outcomes framework links those outcomes contained within the mission statement of the Privacy Commissioner with inputs supported by measurable service performance standards.

Outcomes in the short and long term



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	3,248	3,248
Other Revenue	301	395
Total Revenue	3,549	3,644

STATEMENT OF OBJECTIVES AND SERVICE PERFORMANCE

FOR THE YEAR ENDED 30 JUNE 2013

	Actual 2013 $000	Budget 2013 $000
OUTPUT 1:		
Awareness and Compliance		
Resources employed		
Revenue	1,556	1,515
Expenditure	1,509	1,531
Net Surplus(Deficit)	**47**	**(16)**
OUTPUT 2:		
Government and Business		
Resources employed		
Revenue	1,384	1,348
Expenditure	1,334	1,353
Net Surplus(Deficit)	**50**	**(5)**
OUTPUT 3:		
New technologies and international connections		
Resources employed		
Revenue	704	685
Expenditure	665	677
Net Surplus(Deficit)	**39**	**9**

TOTALS:		
Resources employed		
Revenue	3,644	3,549
Expenditure	3,508	3,561
Net Surplus(Deficit)	**136**	**(12)**

Output 1 – Awareness and Compliance

New Zealanders recognise the individual and societal value in protecting privacy.

Why is this important?

There is an increasing public awareness of privacy and privacy rights as a general issue, but this awareness remains relatively unsophisticated. The Office has experienced a trend of increasing numbers of media and public enquiries, and complaints over the past five years.

As awareness of privacy increases, this places further demand on the Office for perspectives and guidance on the key issues. Faced with resource pressures, we will require different ways of exerting influence over awareness and individual behaviour.

The impacts we seek

- Individuals empowered to take ownership of, and self-resolve privacy issues.
- Individuals and organisations are able to access information about privacy rights.

Quantity	Achievement
Organise the annual New Zealand Privacy Awareness Week as part of Asia-Pacific Privacy Awareness Week.	Achieved Privacy Awareness Week ran from 28 April – 4 May. Our major event was the data safety workshop on 1 May, and we assisted in developing the APPA infographic - a joint international promotional product.
Provide education activities to public and private organisations to facilitate an understanding of their obligations under the Privacy Act.	Achieved (new measure in 2012/13) The Office provides an education workshop programme throughout the year. In addition we undertake presentations and other public seminars.
Provide an enquiries service including 0800 helpline and website access to information, supporting self-resolution of complaints.	Achieved (2011/12 Achieved 8,468 received) The 0800 line received 9,038 enquiries. Both the enquiries 0800 line and the website were fully operational throughout the year. New strategy introduced to involve a greater level of supporting staff involvement to provide broader coverage and support.

Quantity	Achievement
Prepare practical guidance materials to assist public awareness and understanding of the Privacy Act.	Achieved (2011/12 Achieved) Our major product was the cloud computing guidance. http://privacy.org.nz/how-to-comply/using-the-cloud/
Maintain an effective website and other publications to assist stakeholders to promote better privacy practice.	Achieved (2011/12 Achieved) The website is regularly updated. The website platform was also enhanced this year (moved onto SilverStripe Express), with some additional functionality and security, and to guarantee continued IT support.
Respond to media enquiries.	Achieved (new measure in 2012/13) Media enquiries all separately logged, with responses. Media enquiries received for the year were 310..
Provide a robust complaints and investigation service.	Achieved (new measure in 2012/13) Settlement rates increased. Timeliness maintained and those complaints with little chance of success are identified early and given appropriate attention.

Activities	Estimation	Achieved
Education workshops delivered	35	36
Presentations at conferences / seminars	15	70
Estimated number of enquiries received and answered	6,000	9,038
Media enquiries received	250	310
Number of complaints received	900	824
Number of current complaints processed to completion or settled or discontinued	900	896

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 (2011/12 Not achieved) 70% of complainants' and respondents' satisfaction with the complaints handling process rated as "satisfactory" or better. The response rate to the survey has been reducing over recent years. The small response rate means that any minor change may result in a significant movement in the final results. 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. 50% of complainants and 90% 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. A breakdown of responses is provided in the Annual Report 2013.
Of the complaints processed, 30% are closed by settlement between the parties.	Achieved (2011/12 Achieved) 36% of complaints were closed by settlement (2011/12 was 30.3%)
In 90% of the complaints closed, we demonstrate personal contact, either by phone or in person, with one or more of the parties.	Not achieved (2011/12 Not achieved) Achieved 69%. The increased number of complaints received impacts on target of 90%. The goal is being reassessed in line with continued growth in complaints workload.
An external review of a sample of complaints investigations demonstrates an acceptable standard of the legal analysis, correctness of the legal conclusions, soundness of the investigative procedure and timeliness of response.	Achieved (new measure in 2012/13) An independently assessed sample of 20 files each scored out of 5 attained an average of 3.8 per file. It indicates complaints investigations achieved an acceptable standard of the legal analysis, correctness of the legal conclusions, soundness of the investigative procedure and timeliness of response.
Evaluations show that the expectations of 90% of attendees at workshops were either met or exceeded for the quality of presentations.	Achieved (2011/12 Achieved) The overall percentage achieved is calculated as a percentage of the attendees and measure their expectations in attending the workshop with 99% having expectations met or exceeded. 82% of attendees who completed the evaluation rated the presenter Very Good or Excellent, while 79% rated the materials Very Good or Excellent.
Case notes are published in accordance with standards adopted by the Asia Pacific Privacy Authorities (APPA) forum.	Achieved (2011/12 Achieved 11 case notes published). 9 case notes published during the year.

Quality	Achievement
Website publications provide reliable and relevant information which is legally accurate and in plain English.	Achieved (2011/12 Achieved) For example, see the cloud computing guidance: http://privacy.org.nz/how-to-comply/using-the-cloud/

Timeliness	Achievement
80% of complaints are completed, settled or discontinued within nine months of receipt.	Achieved (2011/12 Achieved 95%) 93% of complaints were completed, settled or discontinued. 17% of open complaints at year end were greater than nine months of receipt
Report on all operating information matching programmes in the Annual Report.	Achieved (2011/12 Achieved) Reports on all information matching programmes are published in the Annual Report of the Privacy Commissioner.
Current information is placed on the website within five working days of being made available.	Achieved (2011/12 Achieved) Usually same day publication, or within a day or two depending on staff availability.
Respond to 90% of 0800 line enquiries within one working day.	Achieved (2011/12 Achieved 96%) 94% of enquiries were responded to within one working day.
Respond to 70% of phone enquiries live.	Not achieved (new measure in 2012/13) A new performance measure with an ambitious target. 66% of phone enquiries were answered live. Not achieved due to process faults and capacity issues. Changes currently being made to improve process and capacity.
All media enquiries are recorded and responded to within agreed deadlines.	Achieved (new measure in 2012/13) The Office responded to 310 media enquiries. A separate record of each media enquiry is maintained in Objective. If there is a deadline, this is noted.

OUTPUT 2 – GOVERNMENT AND BUSINESS

Achieve excellence in personal information handling by government and business.

Why is this important?

Government and business hold large amounts of New Zealanders personal information. Evidence from the Office's own research, and from analysis of the complaints it receives, provides stark evidence that some agencies continue to make basic and avoidable mistakes in handling personal information. While there are some organisations that have very good privacy practices, a high standard of privacy practice is not widespread. Poor privacy practices and information handling by government and business is the major threat to New Zealanders' privacy.

The impacts we seek

- Agencies are better able to manage harm arising from a privacy breach.
- Privacy by Design is widely applied by business and government.
- Provision of public services has minimal impact on New Zealanders' privacy.

Quantity	Estimation	Achieved	2011/12
Projected number of active information matching programmes monitored	52	54	50

Quantity	Achievement
Provide assistance to promote better privacy practice in business and government.	Achieved (new measure in 2012/13) For instance, we have been involved in many of the information governance discussions across government, and we published our guidance on cloud computing for SMEs.
Issue and keep current codes of practice.	Achieved (new measure in 2012/13) The Office issued one new code - the Civil Defence National Emergencies (Information Sharing) Code 2013. There has been on-going work on the Credit Reporting Privacy Code including updates coming into force. We also amended the Health Information Privacy Code to take into account the legislative changes in the main Act relating to serious risks to safety.
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 (2011/12 Achieved 115) 58 new policy files were 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 (2011/12 Achieved) Contact with departments as required under applicable memoranda of understanding. Formal reporting through the agreed Ministry of Health work plan. Internal Affairs has no detailed work plan but there have been regular meetings and substantial work done (e.g. on Electronic Identification and Verification Service).

Quantity	Achievement
Privacy breach guidelines for agencies are available to government and business.	Achieved (new measure in 2012/13) Privacy breach guidelines are published on our website. The guidelines are well known, often used and referred to in many of the breach notifications that we receive.

Quality	Achievement
Assistance provided to government agencies presents a clear, concise and logical argument, and is supported by facts.	Achieved (2011/12 Achieved) Assistance is recorded in policy files. On-going 'Plain English' training received by the policy team has also assisted in clarity of communication.
Respond to feedback obtained from recipients of policy advice.	Achieved (2011/12 Achieved) Feedback is sought to our reports and it is through consultation that the final reports are developed.
All proposals for codes of practice will be the subject of discussion with stakeholders and, where required, a public consultation process.	Achieved (new measure in 2012/13) Submissions are sought from interested parties by use of the public notices section of the major newspapers and by a notice on our website.
All issued codes of practice are referred to the Regulations Review Committee of the House of Representatives.	Achieved (new measure in 2012/13) The Civil Defence National Emergencies (Information Sharing) Code 2013 was referred to the Regulations Review Committee.
Provide all draft reports on operating, information matching programmes to the relevant departments for comment before they are published in the Annual Report.	Achieved (2011/12 Achieved) All relevant departments receive a draft report of their authorised information matching programmes for comment, prior to publication in our Annual Report.
Reports on information sharing are reported in the Annual Report.	Achieved (2011/12 Achieved) Reports on all information matching programmes are published in our Annual Report.
Statutory responsibilities are met.	Achieved (new measure in 2012/13) For example, we have completed several section 106 reports (periodic reviews of information matches)

Timeliness	Achievement
Advice given to agencies by the agreed date so that it is useful to them.	Achieved (2011/12 Achieved) This was despite sometimes very tight turn-around times placed on us by agencies.
Report on all operating information matching programmes within the Annual Report.	Achieved (new measure in 2012/13) Reports for the previous year were available in the 2011/12 Annual Report.
Formal response deadlines are met.	Achieved (new measure in 2012/13)
Statutory timeframes are met.	Achieved (new measure in 2012/13)

OUTPUT 3 - NEW TECHNOLOGIES AND INTERNATIONAL CONNECTIONS

New Zealanders' privacy is resilient in the face of the changing privacy demands of the electronic age.

Why is this important?

Technological change and the future application of technology are not entirely predictable trends, although the rapid pace of change is well-recognised.

Often new technologies and applications are developed and put into use before the privacy implications are fully understood. Existing regulatory frameworks were not established with the IT revolution fully in mind. The pace of change poses a real challenge for maintaining the relevance of the regulatory framework in privacy knowledge and practice.

There is an expectation that the Privacy Commissioner in her role as a privacy watchdog is able to quickly develop a view on the privacy implications of new technology and its use. For the Office to remain credible and effective over time, it needs to be very good at scanning emerging developments, selecting the issues that require a proactive response, and moving quickly to develop an appropriate response.

The impacts we seek

- Barriers to business and investment lowered by close co-operation across international jurisdictions.
- Businesses, government and individuals are able to take advantage of new technologies while respecting privacy.
- The Privacy Act recognised as meeting the requirements of our trading partners.
- Cross-border enforcement laws and practices put in place.

Quantity	Achievement
Participate in international forums.	Achieved (2011/12 Achieved) Participated in Asia Pacific Privacy Authorities (APPA) forum (1 meeting), APEC Data Privacy Subgroup (DPS) (1 meeting), International Conference of Data Protection and Privacy Commissioners (ICDPPC) (1 conference).

Quantity	Achievement
Contribute to international initiatives to facilitate cross-border cooperation in privacy standard setting and enforcement.	Achieved (2011/12 Achieved) Continued as an administrator of the APEC Cross-border Privacy Enforcement Arrangement (CPEA) and as a committee member of the Global Privacy Enforcement Network (GPEN). Participated in an International Enforcement Cooperation Working Group. Sought and obtained approval from APEC Committee on Trade and Investment to run an APEC Privacy Enforcement Workshop. Contributed to updating of OECD privacy guidelines though participation in an experts working group.
Representation at key international forums including the International Conference of Data Protection and Privacy Commissioners (ICDPPC) and the Asia Pacific Privacy Authorities (APPA) forum.	Achieved (new measure in 2012/13) Provided a delegate to each APPA forum (1 of 1 meeting), APEC DPS (1 of 2 meetings) and ICDPPC (1 of 1 conference).
Membership of APEC's Cross-border Privacy Enforcement Arrangement (CPEA) and the Global Privacy Enforcement Network (GPEN).	Achieved (new measure in 2012/13) The Office is a participant in both the APEC CPEA and GPEN and is represented on the governance committees of both enforcement networks.
Undertake research into, and to monitor developments in, privacy related technologies.	Achieved (new measure in 2012/13) Cloud computing was the main focus during the year, including finalising our guidance material.

Quality	Achievement
New Zealand remains in consideration to achieve an 'adequacy finding' from the European Union.	Achieved (2011/12 Achieved) The European Commission took a formal decision in December to recognise that New Zealand law provides an adequate level of data protection.
Participation is valued by international colleagues and our contribution is influential.	Achieved (2011/12 Achieved) Continued in role on governance committees of CPEA and GPEN. Continued to receive invitations to speak at international events. Approved by APPA and APEC to host future events on their behalf.
Technology research projects and their findings are presented to a public forum.	Achieved (new measure in 2012/13) Four technology and privacy forums were undertaken during the year.

Timeliness	Achievement
Advice given to international jurisdictions within the agreed timeframes.	Achieved (2011/12 Achieved) All applicable deadlines observed (e.g. to submit comments during review of OECD privacy guidelines).
Provide reports and updates on technology related research within the agreed timeframes.	Achieved (new measure in 2012/13) Cloud computing guidance materials published.

STATEMENT OF ACCOUNTING POLICIES
FOR THE YEAR ENDED 30 JUNE 2013

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 New Zealand 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 (NZIFRS).

The financial statements for the Privacy Commissioner are for the year ended 30 June 2013, and were approved by the Commissioner on 30 October 2013. 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 (NZGAAP).

The financial statements comply with NZIFRSs, 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, IRD is included as part of receivables or payables in the statement of financial position.

The net GST paid to, or received from 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 and the 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 end 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 ANZ 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 2013:

Leases classification

Determining whether a lease agreement is a finance or 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 NZIAS 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. The Privacy Commissioner would present this analysis in note 6.
- FRS-44 *New Zealand Additional Disclosures and Amendments to NZIFRS 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. There is not expected to be any significant effect for the Privacy Commissioner as the Office does not revalue assets.

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:

- NZIFRS 9 *Financial Instruments will eventually replace NZIAS 39 Financial Instruments: Recognition and Measurement.* NZIAS 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 NZIFRS 9. NZIFRS 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 NZIAS 39. The approach in NZIFRS 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 NZIAS 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 2016. However, as a new accounting standards framework will apply before this date, there is no certainty when an equivalent standard to NZIFRS9 will be applied to public benefit analysis.

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, the Privacy Commissioner 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 f94%or the new standards for public sector entities is expected to be for reporting periods beginning on or after 1 July 2014. This means the Privacy Commissioner expects to transition to the new standards in preparing its 30 June 2015 financial statements. As the PAS are still under development, the Privacy Commissioner 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 NZIFRS and amendments to existing NZIFRS 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 NZIFRS that exclude public benefit entities from their scope.

STATEMENT OF COMPREHENSIVE INCOME

FOR THE YEAR ENDED 30 JUNE 2013

	Note	Actual 2013 $000	Budget 2013 $000	Actual 2012 $000
Revenue				
Crown revenue	2	3,248	3,248	3,248
Other revenue	3	361	266	312
Interest		34	35	35
Total income		3,643	3,549	3,595
Expenditure				
Promotion	4	57	53	49
Audit fees		27	18	24
Depreciation and amortisation	1, 10, 11	142	150	114
Rental expense		395	420	401
Operating expenses		370	420	371
Staff expenses	5	2,517	2,500	2,508
Total expenditure		3,508	3,561	3,467
Surplus/(deficit)		136	(12)	128
Other comprehensive income		-	-	-
Total comprehensive income		**136**	**(12)**	**128**

STATEMENT OF CHANGES IN EQUITY

FOR THE YEAR ENDED 30 JUNE 2013

	Note	Actual 2013 $000	Budget 2013 $000	Actual 2012 $000
Total equity at the start of the year		656	430	528
Operating surplus for the period		136	-12	128
Total recognised revenue and expenses for the period		136	-12	128
Total equity at the end of the year	**6**	**792**	**418**	**656**

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

STATEMENT OF FINANCIAL POSITION

AS AT 30 JUNE 2013

	Note	Actual 2013 $000	Budget 2013 $000	Actual 2012 $000
Public equity				
General funds	6	792	418	656
Total public equity		792	418	656
Current assets				
Cash & cash equivalents	7	696	357	469
Debtors and other receivables	8	34	75	16
Inventory	9	8	4	12
Prepayments	8	15	8	29
Total current assets		753	444	526
Non-current assets				
Property, plant & equipment	10	199	149	306
Intangible assets	11	52	52	59
Total non-current assets		251	201	364
Total assets		**1,004**	**645**	**890**
Current liabilities				
Creditors and other payables	12	103	146	106
Employee entitlements	13	109	80	127
Total current liabilities		212	226	233
Total liabilities		212	226	233
Net assets		**792**	**419**	**657**

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

STATEMENT OF CASH FLOWS

FOR THE YEAR ENDED 30 JUNE 2013

	Note	Actual 2013 $000	Budget 2013 $000	Actual 2012 $000
Cash flows from operating activities				
Cash was provided from:				
Supply of outputs to the Crown		3,454	3,248	3,255
Revenues from services provided		150	266	312
Interest received		34	35	35
Cash was applied to:				
Payment to suppliers		835	911	879
Payments to employees		2,535	2,500	2,490
Net goods and services tax		11	15	116
Net cash flows from operating activities	14	257	123	117
Cash flows from investing activities		-	-	-
Cash was provided from:				
Landlord's capital contribution		-	-	-
Cash was applied to:				
Purchase of property plant and equipment		30	110	254
Purchase of intangible assets		-	-	-
Net cash flows from investing activities				-
Net increase (decrease) in cash held		227	13	(137)
Plus opening cash		468	344	606
Closing cash balance		696	357	469
Cash and bank		696	357	469
Closing cash balance		**696**	**357**	**469**

The GST (net) component of operating activities reflects the net GST paid and received with IRD. 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

NOTES TO THE FINANCIAL STATEMENTS

FOR THE YEAR ENDED 30 JUNE 2013

Note 1: Total Comprehensive Income

	Actual 2013 $000	Actual 2012 $000
The total comprehensive income is after charging for:		
Fees paid to auditors		
External audit	-	-
Current year	27	24
Prior year	24	23
Depreciation:		
Furniture & fittings	78	62
Computer equipment	57	40
Office equipment	7	7
Total depreciation for the year	142	109
Amortisation of intangibles		2
Rental expense on operating leases	395	401

Major budget variation

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

Statement of comprehensive income

Other revenue / operating expenses

The Privacy Commissioner held a privacy workshop as part of Privacy Awareness Week. The attendance exceeded expectations and a profit of $21,626 was achieved. The Office received $60,000 sponsorship to host the APEC-Cross-border Privacy Enforcement Arrangement (CPEA) meeting and Asia Pacific Privacy Authorities (APPA) meeting both being held in July 2013. The costs of the meetings will be incurred in the first quarter of 2013/14 year.

Savings in the order of $50,000 were made in the area of domestic and international travel.

Staff expenses

Parental leave contributed to a reduction in staff expenses. The roles were specialised positions and could not be effectively replaced by temporary staff for the duration of the parental leave.

There was staff turnover in the last quarter of the year which resulted in further savings in salaries.

The savings were then offset by the impacts of KiwiSaver entitlements, the result being that staff expenses exceeded budget.

Surplus

The surplus was largely the result the additional other revenue and a reduction in operating expenses.

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 (2012: $nil).

Note 3: Other revenue

	Actual 2013 $000	Actual 2012 $000
Other grants received	206	206
Rental income from property sub-leases	25	25
Privacy forum	22	40
Seminars & workshops	43	39
Other	67	2
Total other revenue	**363**	**312**

Note 4: Promotion expenses

	Actual 2013 $000	Actual 2012 $000
Website development expenses	20	2
Publications	4	17
Inventories consumed	-	-
Privacy forum	10	21
Other marketing expenses	23	9
Total marketing expenses	**57**	**49**

Note 5: Staff expenses

	Actual 2013 $000	Actual 2012 $000
Salaries and wages	2,334	2,335
Employer contributions to defined contribution plans	76	43
Other staff expenses	27	25
Other contracted services	96	87
Increase/(decrease) in employee entitlements	(16)	18
Total staff expenses	**2,517**	**2,508**

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

Prior components of staff expense have been reclassified to provide consistency with current year disclosure with no change in total staff expense.

Note 6: General funds

	Actual 2013 $000	Actual 2012 $000
Opening balance	656	528
Net (deficit) / surplus	136	128
Closing balance	**792**	**656**

Note 7: Cash and cash equivalents

	Actual 2013 $000	Actual 2012 $000
Cash on hand and at bank	31	48
Cash equivalents – on call account	665	421
Total cash and cash equivalents	**696**	**469**

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 2013 $000	Actual 2012 $000
Trade debtors	33	16
Prepayments	15	29
Total	**48**	**45**

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 (2012: $nil).

Impairment

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

Aging analysis:	2013 $000	2012 $000
Not past due		14
Past due 1-30 days	7	2
Past due 31-60 days	0.05	
Past due 61-90 days	1	
Past due >91 days	0.2	
Total debtors and other receivables	**8**	**16**

As at 30 June 2013, no debtors have been identified as insolvent. (2012 $nil).

Note 9: Inventories

	Actual 2013 $000	Actual 2012 $000
Publications held for sale	**8**	**12**

The carrying amount of inventories held for distribution that are measured at current replacement cost as at 30 June 2013 amounted to $nil (2012: $nil).

There have been no write-down of inventories held for distribution or reversals of write-downs (2012 $nil).

No inventories are pledged as security for liabilities (2012: $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 2011	415	214	116	745
Additions	-	164	26	190
Disposals	-	(89)	(47)	(136)
Balance at 30 June 2012	415	289	95	799
Balance at 1 July 2012	415	289	95	799
Additions	0	12	6	18
Disposals	0	(53)	(30)	(83)
Balance at 30 June 2013	**415**	**248**	**71**	**734**
Accumulated depreciation and impairment losses				
Balance at 1 July 2011	249	160	111	520
Depreciation expense	62	40	7	109
Disposals	-	(89)	(47)	(136)
Balance at 30 June 2012	311	111	71	493
Balance at 1 July 2012	311	111	71	493
Depreciation expense	60	57	7	124
Elimination on disposal		(53)	(30)	(83)
Balance at 30 June 2013	**371**	**116**	**47**	**534**
Carrying amounts				
At 1 July 2012	103	177	24	305
At 30 June 2013	**43**	**132**	**24**	**199**

Note 11: Intangible assets

Movements for each class of intangible asset are as follows:

	Acquired software $000
Cost	
Balance at 1 July 2011	283
Additions	62
Balance at 30 June 2012	345
Balance at 1 July 2012	345
Additions	11 (283)
Balance at 30 June 2013	**73**
Accumulated amortisation and impairment losses	
Balance at 1 July 2011	281
Amortisation expense	5
Balance at 30 June 2012	286
Balance at 1 July 2012	286 (283)
Amortisation expense	18
Balance at 30 June 2013	**21**
Carrying amounts	
At 1 July 2011	2
At 30 June and 1 July 2012	59
At 30 June 2013	**52**

There are no restrictions over the title of the Privacy Commissioner's intangible assets, nor are any intangible assets pledged as security for liabilities.

Note 12: Creditors and other payables

	Actual 2013 $000	Actual 2012 $000
Creditors	34	46
Accrued expenses	68	60
Other payables		-
Total creditors and other payables	**103**	**106**

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 2013 $000	Actual 2012 $000
Current employee entitlements are represented by:		
Accrued salaries and wages	-	3
Annual leave	109	125
Total current portion	**109**	**128**
Current	109	128
Non-current	-	-
Total employee entitlements	**109**	**128**

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

	Actual 2013 $000	Actual 2012 $000
Total comprehensive income	**136**	**128**
Add/(less) non-cash items:		
Depreciation and amortisation	142	114
Other non-cash Items	-	-
Total non-cash items	**142**	**114**
Add/(less) movements in working capital items:		
Increase/(decrease) in creditors	(12)	(21)
Increase/(decrease) in accruals	8	(20)
(Increase)/decrease in inventory	3	9
Increase/(decrease)in payables		(98)
Increase/(decrease)in employee entitlements	(18)	18
Increase/(decrease) in income in advance	-	-
(Increase)/decrease in receivables	(2)	(13)
Working capital movements - net	**(21)**	**(125)**
Add/(less) items classified as investing activities:	-	-
Landlord's capital contribution	-	-
Total investing activity items	-	-
Net cash flow from operating activities	**257**	**117**

Note 15: Capital commitments and operating leases

Capital commitments

The Privacy Commissioner has no capital commitments for the year. (2012: $nil)

Operating leases

	Actual 2013 $000	Actual 2012 $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	295	355
Later than one year and not later than five years	833	556
Later than five years	137	-

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 expire 31 July 2013. The Privacy Commissioner entered into a new lease on the existing Auckland premises prior to year end and being effective from 1 August 2013 to 31 July 2019.

Total future minimum sublease payment to be received under non-cancellable subleases for office space at the balance date including six month notice period is $14,427 (2011: $26,793). With the new lease, the sub-lease has also with recognition of six months commitment under the sub-lease.

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

Note 16: Contingencies

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 (2012: $nil).

Note 17: Related party information

The Privacy Commissioner is a wholly owned entity of the Crown. The Government significantly influences the role of the 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 the Trust during the current financial year (In 2012, 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 2013 $000	Actual 2012 $000
Total salaries and other short-term employee benefits	**883**	**870**

Key management personnel include all senior management team members and the Privacy Commissioner who together comprise the leadership team.

Note 18: 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 2013	Actual 2012
$100,000 - $109,999	1	-
$110,000 - $119,999	-	-
$120,000 - $129,999	-	-
$130,000 - $139,999	-	2
$140,000 - $149,999	2	1
$150,000 - $159,999	1	-
$160,000 - $169,999	1	1
$270,000 - $279,999	-	1
$280,000 - $289,999	1	-

Note 19: Commissioner's total remuneration

In accordance with the disclosure requirements of Section 152 (1)(a) of the Crown Entities Act 2004, the total remuneration includes all benefits paid during the period 1 July 2012 to 30 June 2013.

Name	Position	Amount 2013	Amount 2012
Marie Shroff	Privacy Commissioner	$284,177	$278,469

Note 20: Cessation payments

No redundancy payments were made in the year. (2012: $nil)

Note 21: Indemnity insurance

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

Note 22: 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 23: Financial instruments

21A Financial instrument categories

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

	2013 $000	2012 $000
FINANCIAL ASSETS		
Loans and receivables		
Cash and cash equivalents	696	469
Debtors and other receivables	34	16
Total loans and receivables	730	485
FINANCIAL LIABILITIES		
Financial liabilities at amortised cost		
Creditors and other payables	103	106
Total financial liabilities at amortised cost	**103**	**106**

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 2013 (2012: $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 has no interest-bearing liabilities. The Privacy Commissioner invests cash and cash equivalents with ANZ, ensuring a fair market return on any cash position, but does not seek to speculate on interest returns, and does 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 ANZ will fluctuate because of changes in market interest rates. The Privacy Commissioner does not consider that there is any significant interest exposure on the Privacy Commissioners investments. The Privacy Commissioner is primarily exposed to changes in the New Zealand dollar official cash rate.

Interest rate exposure – maturity profile of financial instruments

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

	Weighted average effective interest rate	Variable interest rate	Fixed maturity dates – less than 1 year	Non-interest bearing
2013	%	NZ$000	NZ$000	NZ$000
Financial assets				
Cash and cash equivalents	-	696	-	-
	-	**696**	**-**	**-**
2012				
Financial assets				
Cash and cash equivalents	-	469	-	-
	-	**469**	**-**	**-**

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 Privacy Commissioner and represents the Commissioner's assessment of a reasonably possible change in interest rates.

	Net surplus 2013 NZ$000	Net surplus 2012 NZ$000
Cash and cash equivalents +100 bps	5.43	4.90
Cash and cash equivalents – 100 bps	(5.43)	(4.90)

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