PRIVACY COMMISSIONER

ANNUAL REPORT 2014

Privacy Commissioner
Te Mana Matapono Matatapu

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

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

Annual Report of the Privacy Commissioner

For the year ended 30 June 2014

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

November 2014

THE MINISTER OF JUSTICE

I tender my report as Privacy Commissioner for the year ended 30 June 2014

John Edwards

Privacy Commissioner

CONTENTS

TABLES AND FIGURES

APPENDICES

1. KEY POINTS

Outreach and communications

- Our regular UMR survey in March 2014 showed the highest level of public concern about privacy and personal information handling since the survey began in 2001. Half of all New Zealanders say they have become 'more concerned' about privacy issues over the past few years.
- We received over 8,000 enquiries from members of the public and organisations seeking guidance on privacy matters.
- We received 287 media enquiries covering a wide range of topics, including the GCSB Bill and surveillance related issues; the debate about an individual's right to be forgotten; the new Privacy Commissioner; and upcoming privacy law reforms.
- The Office began a blog in 2014, enabling us to provide current news, updates and comments on a range of privacy topics.
- The Commissioner and senior staff delivered 59 speeches and presentations during the year to a wide range of audiences.
- The Office delivered 39 training and education workshops and seminars to members of the public and stakeholder groups.
- We appointed a full-time communications adviser, enhancing our ability to respond to media requests and to develop our social media and website content.

Complaints and investigations

- We received 725 complaints from members of the public.
- We completed a joint investigation with the Ombudsman on the Earthquake Commission's (EQC) handling of information requests in the aftermath of the Canterbury earthquakes. The report found EQC had failed to comply with its Official Information Act and the Privacy Act obligations to provide information to requesters in a timely manner. EQC accepted the recommendations and took steps to implement them.
- The Office conducted an own motion investigation into credit reporter Veda Advantage's charge for urgent requests by consumers for access to their own credit information. The investigation concluded that Veda's charge of $51.95 for urgent requests was unreasonable and unlawful. Veda failed to provide adequate assurances that it would act reasonably so the Credit Reporting Privacy Code was amended to enforce compliance. The Credit Reporting Privacy Code was amended accordingly and Veda has complied with the change.

Policy and technology

- The Government accepted the major Law Commission's recommendations for change to the Privacy Act. We continued to work closely with Ministry of Justice officials on the reforms and in the drafting of a new Privacy Bill.
- We made a submission to the Social Services select committee on the proposal to create Child Harm Prevention Orders within the Vulnerable Children Bill.
- We supported the work of the New Zealand Data Futures Forum in its efforts to build a strategic vision for

New Zealand's digital future.

- The Government Chief Privacy Officer role was established during the year and the Office is collaborating closely in furthering our complementary aims.
- The first two information sharing agreements under the Privacy Amendment Act 2013 were authorised. They are between Inland Revenue - Department of Internal Affairs, and between Inland Revenue - New Zealand Police.
- The Office gained an advisory position in the National Health IT Board's Health Information Governance Expert Advisory Group. The Advisory Group is working to develop a Health Information Governance Framework.
- The Office has reviewed and reported on three electronic health record initiatives to assess how they dealt with privacy issues. The report is available on our website at www.privacy.org.nz.
- We made a submission to the Privileges Committee on the Inquiry regarding the use of intrusive powers within the Parliamentary precinct.
- We provided a submission to MBIE on the NZ Business Number Programme.
- The Office released best practice guidance for app developers during the year. It is available at www.privacv.org.nz .

Data breaches

- We continued to receive a regular stream of data breach notifications throughout the year. We have noticed a growing responsiveness by business and government to the reputational benefits of notifying clients when things go wrong.
- Government organisations continue to make up the largest single sector reporting data breaches. The health and business sectors were also significantly represented. (See further detail on page 19).
- The most common types of breaches notified were electronic or physical information sent to the wrong recipients.

International

- In July 2013, we hosted the 39th Asia Pacific Privacy Authorities forum in Auckland and participated in the 40th and 41st forums in Sydney and Seoul. The APPA Forum is continuing to build its importance in the region. Singapore is the most recent authority to join.
- At the same gathering, we hosted an APEC Data Privacy Subgroup capacity building workshop. The event drew more than 70 participants from 15 APEC economies as well as Europe and other regions.
- New Zealand's law currently provides an 'adequate level of data protection' for the purposes of existing EU law. However, the EU law is now under review and due to be replaced by new regulations. We continued efforts to ensure that European officials understand the need for a smooth transition of these adequacy decisions into any new regime.
- In May 2014, we participated in the Global Privacy Enforcement Network (GPEN) Mobile App Sweep; an internationally coordinated effort to scan mobile apps to assess the adequacy of their privacy notices and policies. The international findings were that nearly one third (31%) of all mobile apps raise concerns about the nature of permissions sought. New Zealand findings were broadly consistent with 38% of mobile apps raising concerns.

2. INTRODUCTION

Law reform

A major landmark in the year was the Government's decision to reform the Privacy Act. Cabinet announced its intention in May 2014, and adopted most of the Law Commission's recommendations for revitalising the Act.

We support most of those Cabinet decisions. The reforms will make many of the Act's processes more efficient, and will promote and protect individual privacy without stifling legitimate business interests or innovation. They will bring the Privacy Act more up to date with the current technological and international environment.

Key reforms include:

- giving the Privacy Commissioner the power to order agencies to comply with the law
- giving the Privacy Commissioner the power to order agencies to provide personal information to requesters where there is no lawful basis for withholding it
- clarifying agencies' responsibilities when they send information offshore
- creating a legal responsibility to report material data breaches to our office, and also to report serious breaches to affected individuals.

Emerging debates

Privacy has continued to be a prominent subject of public debate and discussion both domestically and internationally. For instance, revelations attributed to the former US National Security Agency employee Edward Snowden put a global focus on online surveillance. This had repercussions in New Zealand by highlighting the role of the Government Communications Security Bureau at a time when the law governing its activies was being reformed. The heightened public awareness and interest in the activity of security and intelligence agencies has led the Office to explore options for enhanced cooperation between oversight agencies.

International surveillance activities are one part of a highly dynamic picture. Information privacy and data protection has developed rapidly against a background of technology changes such as the growth in cloud computing; mobile computing; social networking; cross-border data transfers; biometrics; data analytics; online fraud, and the capabilities of technology such as unmanned aerial vehicles (UAVs).

More recently, in New Zealand, we have seen active debates over the way personal information has been handled by bloggers and others on social media. We can readily find examples where individuals have been harmed by hacked or improperly obtained information being widely distributed to the public. New Zealanders are perhaps becoming more critical of the provenance of information and more aware its misuse. There is no doubt that these debates illuminate the need to clarify the legal boundaries and to ensure the protection of the law can be extended to everyone.

Public opinion

Our own research in a UMR survey conducted at the beginning of 2014, shows that New Zealanders are more concerned about privacy, especially about whether their personal information is well managed and protected. The survey showed that half of all participants say they have become 'more concerned' about privacy issues over the past few years. This is a continuation of a trend, and shows the highest level of public concern since the survey began in 2001.

One effect of this changing personal data climate is that government agencies and corporations have found that giving inadequate priority to privacy values can erode trust and confidence, impede the delivery of public services, and wipe out shareholder value.

GCPO

The public sector response to these challenges included establishing a new role of Government Chief Privacy Officer (GCPO). This is a positive development that supports and enhances the regulatory and watchdog functions of the Privacy Commissioner. It reflects an evolving understanding across government of the fact that personal data and information are strategic assets held by government as a steward on behalf of the New Zealand public. We are applying considerable effort and resource to support that role and to minimise role confusion and duplication.

Capacity building

The 2014 budget provided much needed additional funding for OPC through Vote Justice. This increase to baseline funding reflects changing demands upon the Office over a number of years and the fact that good information privacy practice is integral to the success of Better Public Services, especially Key Result Areas 4, 9 and 10.

We will be making these areas a priority in our ongoing work:

- building capacity in the market for privacy expertise
- supporting Better Public Services initiatives
- developing comprehensive and clear guidance to help businesses and individuals comply with the law and prepare for law changes
- continuing to collaborate with international colleagues to achieve effective enforcement outcomes
- monitoring and developing guidance on Authorised Information Sharing Agreements (AISAs)
- working with the Vulnerable Children's Board, Child Protection Teams and the Children's Commissioner and others to resolve information sharing dilemmas arising in the context of care plans for vulnerable children
- developing our public outreach programme through redeveloping our website and online resources, and targeting areas of identified need; and
- enhancing our enforcement and dispute resolution processes, for instance by:
    - greater use of powers such as compulsory conferences
    - introduction of clear policy around naming agencies; and
    - maintaining a strong resolution focus.

3. REPORT ON ACTIVITIES

International activities

There is an underlying international dimension to many aspects of information privacy. Most significant is the cross-border transfer of personal information that is now a routine feature of business and personal life.

Global privacy enforcement authorities need to cooperate across borders to protect against privacy threats wherever they originate. Collaboration with counterpart authorities can lead to enhanced problem solving, creative policy solutions and more effective regulation.

We engage with overseas counterparts in a number of ways. For example:

- developing common standards to facilitate business transactions across borders in ways that protect the interests of individuals;
- seeking the cooperation of overseas enforcement authorities in responding to a security breach;
- gaining 'advance warning' of privacy challenges through the experience of other countries.

We engage in a variety of forums, principally:

- 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, Singapore and the United States
- International Conference of Data Protection and Privacy Commissioners: brings together nearly 100 authorities from around the world
- Asia Pacific Economic Co-operation (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
- Organisation for Economic Co-operation and Development (OECD): the Working Party on Security and Privacy in the Digital Economy (SPDE) draws upon privacy expertise from across OECD countries to advance public policy objectives.

Highlights

Some of the highlights of 2013/14 were:

European Union: The European Commission reached the decision in December 2012 that New Zealand's law provides an 'adequate level of data protection' for the purposes of existing EU law. The EU law is now under review and due to be replaced by new regulations. As a result, we continued efforts, sometimes together with colleagues from other 'adequate' third countries, to ensure that European officials understood the need for a smooth transition of these adequacy decisions into any new regime.

APPA Forum: we hosted the 39th forum in Auckland in July 2013 and participated in the 40th and 41st forums in Sydney and Seoul. The APPA Forum continues to build its importance in the region. Singapore is the most recent authority to join.

Global Privacy Enforcement Network (GPEN): we continued to help lead the network through participation on the GPEN committee. The network has now grown to 47 privacy enforcement authorities in 37 economies. One notable endeavour, led by New Zealand, was the establishment of a monthly GPEN Pacific teleconference where authorities from across the Asia Pacific share experience.

APEC Cross-border Privacy Enforcement Arrangement (CPEA): we continued as a CPEA administrator. This arrangement now connects 24 privacy enforcement authorities in nine APEC economies.

APEC Data Privacy Subgroup: last year we obtained approval from APEC's Committee on Trade and Investment to host a capacity building workshop for privacy enforcement authorities. The two day APEC privacy enforcement workshop was held in Auckland in July 2013 on the fifth anniversary of the APEC CPEA. The event drew more than 70 participants from 15 APEC economies, as well as Europe and other countries.

International Conference of Data Protection and Privacy Commissioners: we proposed a resolution that was adopted, establishing for the first time a strategic direction for the conference. New Zealand was elected for a two year term to the conference's executive committee.

Communications and outreach

Enquiries

We received just over 8,000 individual contacts through our enquiries services – down from over 9,000 the previous year.

Our enquiries service operates a 0800 phone line and an email address. As in previous years, the majority of enquiries were received via the phone (about 75%). Email contact is an increasing area of contact in this channel and fluctuates between a quarter and a fifth of incoming work.

As in the past year, nearly a quarter of all contact was about disclosure or use of personal information. The next largest sector was enquiries about gaining access to information with around 1,600 or a fifth of all contacts.

We don't attempt to gather demographic information from all the enquirers who contact us. Where appropriate, we will record some details about enquirers or who they might represent. The largest group of contacts (over 6,400) was from individuals – reflecting about 80% of all contacts. Other sectors of note were health (about 495), business interests (about 340), government entities (about 140), law firms (about 125) and those generally identified as employers (about 124).

Training and education

This year, we delivered 32 training and education sessions which in total were attended by about 470 people. Twenty workshops were delivered in Auckland, Wellington and Christchurch. Of those, 11 were an Introduction to the Privacy Act and nine focused on the Health Information Privacy Code.

Twelve in-house training sessions were delivered to a variety of agencies and included introductions to the Privacy Act and Health Information Privacy Code.

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

Privacy Week (4 - 10 May 2014)

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

The focus of Privacy Week 2014 was a half-day privacy forum held in Wellington. GCSB Director Ian Fletcher delivered the keynote address. The presentations are available on our website at www.privacy.org.nz.

The Office released its online Data Safety Toolkit during Privacy Week. It is a product in part developed from the previous year's privacy workshop on data breaches.

Every year, APPA members collaborate on a joint product that can be used across the region. For Privacy Week, the Office worked with other APPA members to design a new infographic to be used as a poster or put on an intranet or website.

Presentations

The Commissioner and senior staff delivered 59 speeches and presentations during the year on a range of topics and for a wide variety of audiences. Topics have included:

- The Commissioner's vision as a regulator
- Big data and data analytics
- Cloud computing and identity
- Privacy law reform developments
- The new Government Chief Privacy Officer role.

Online privacy resource for schools

The Office launched a new resource to help teachers teach internet privacy issues to primary and intermediate school students (http://netsafe.org.nz/owls/) at Tawa School in Wellington on 11 February 2014.

The OWLS project was developed with NetSafe in partnership with the NZ National Commission for UNESCO. It is a series of 24 modules on different aspects of managing personal information online. Each module has a lesson plan which teachers can use or adapt to suit their cyber-education classroom needs.

The modules have four themes:

- Own your information: Taking control of information about yourself.
- Wait and think before acting: Taking a moment to think about what you want to do.
- Lock your information: Protecting your information against people who want to steal it.
- Safety: Avoiding some major risks and having back-up plans if things go wrong.

The OWLS resource recognises that schools, teachers and students will have varied experience and knowledge about how to handle personal information. It provides ways for students and teachers to involve families and wider communities.

Blog

The Office began a blog in May 2014. This gives us a new facility to provide news, updates and commentary on a wide range of privacy topics. Staff across the office contribute to the blog and have a by-line. Topics have included comment on the 'right to be forgotten;' the Dirty Politics debate; the High Court's consideration of privacy, and the news media exemption.

Media

The news media made enquiries about a wide range of personal information and technology related topics. The Office received 287 media enquiries during the year.

The GCSB Bill and surveillance related issues were regular subjects of media interest. The scope of the ACC 167 consent form; the Parliamentary inquiry by the Privileges Committee into concerns arising from the release of information relating to a Fairfax journalist and others; and the UMR privacy survey results all contributed strongly to the number of media enquiries received. There was also considerable interest in the upcoming privacy law reforms; the use of drones; the report into charging by the credit reporting company Veda, and the decision by the European Court of Justice into the Right to be Forgotten case against Google.

The Office's ability to respond to media requests, and to assist in providing background information, was greatly eased by the appointment of a full-time communications adviser.

Complaints and access reviews

We received 725 complaints during the year. Table 1 shows incoming and closed complaints and work in progress at year's end.

TABLE 1: COMPLAINTS RECEIVED AND CLOSED 2009–2014

	2009/10	2010/11	2011/12	2012/13	2013/14
Complaints received	978	968	1142	824	725
Complaints closed	961	999	1026	896	702
Work in progress after year's end	290	247	363	291	314

Settlement

Settlement outcomes for this year are shown in Table 2. Of the complaints closed for the year, 32% were closed with some level of settlement. This was a similar result to last year. We achieved some level of resolution in nearly 41% 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. The total number for outcomes listed in the table is higher than the complaints settled as some complaints had multiple settlement outcomes such as an apology, assurances and a monetary payment.

TABLE 2: SETTLEMENT OUTCOMES 2013/14

Settlement outcome	Number
Information released	111
Apology	48
Information partly released	44
Money/monies worth	32
Information corrected	14
Assurances	14
Change of policy	0
Training	5

Complaints received

As in past years, the majority of complaints deal with matters within the information privacy principles in the Privacy Act. Table 3 shows a breakdown between the privacy principles and rules contained in the three codes. Continuing the pattern of previous years, over 60% of our received complaints were from individuals asking us to review the results of access requests they had made to agencies.

TABLE 3: ACT/CODE – BREAKDOWN OF COMPLAINTS RECEIVED 2013/14

(previous year in brackets)

Information Privacy Principle	602 (628)
Health Information Privacy Code	110 (183)
Telecommunications Privacy Code	7 (9)
Credit Reporting Code	6 (4)
TOTAL	725 (824)

Agency types

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

TABLE 4: COMPLAINTS RECEIVED BY AGENCY TYPE 20013/14 (PREVIOUS YEAR IN BRACKETS)

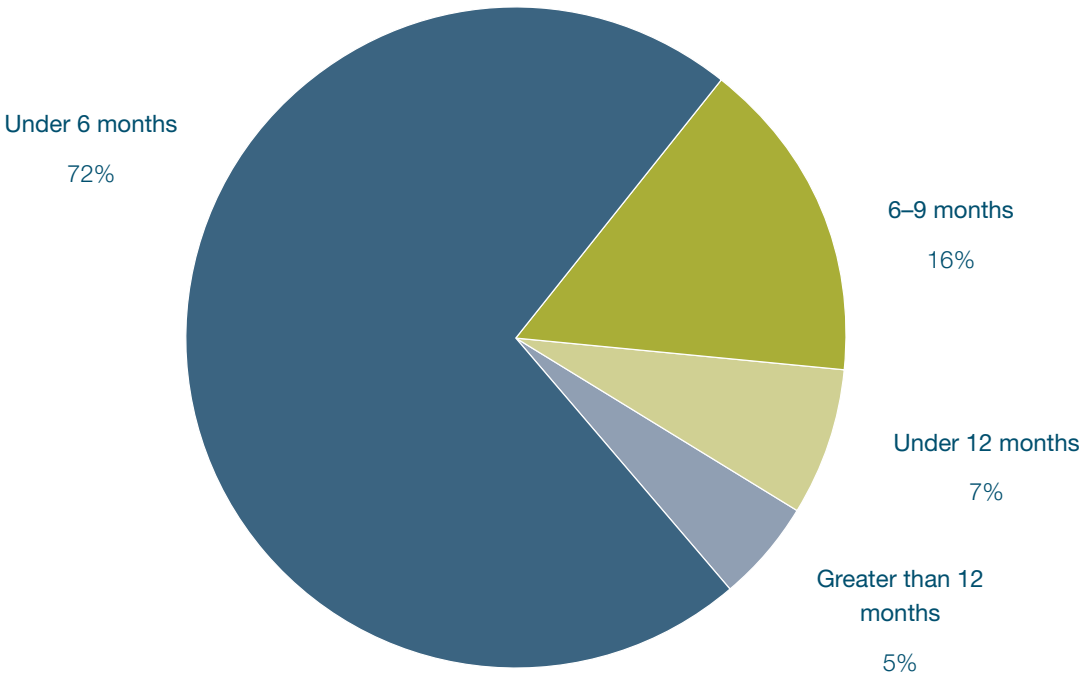
Agency Type	Total	Percentage
Government sector, including education and local authorities	349 (304)	48% (37)
Health sector, including hospitals and medical practices	93 (112)	13% (14)
Financial sector, including banking, insurance, credit agencies and debt collectors	44 (54)	6% (7)
Other	239 (354)	33% (43)
Total	725	100%

Age of complaints

This year, our aim was to complete 80% of our complaint investigations within nine months of receipt. Figure 1 demonstrates that we exceeded our desired outcome by closing 88% within nine months. The remaining 12% mostly involved protracted settlement issues or cases that were complex in nature.

At year's end, work in progress was **314 files of which 89%** were under nine months old. We expect to achieve and continue improvement in our disposition of complaints by refining our techniques and emphasis on dispute resolution.

FIGURE 1: AGE OF CLOSED COMPLAINTS 2013/14



Top respondent agencies

As was the case last 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 six years. It should be noted that the number of complaints received does not necessarily indicate poor practices or systemic failures.

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

TABLE 5: COMPLAINTS RECEIVED AND CLOSED FOR TOP RESPONDENT AGENCIES 2013/14

Agency	No. of complaints received	No. of complaints closed
Department of Corrections	69	46
New Zealand Police	66	63
Ministry of Social Development	40	41
Accident Compensation Corporation	37	33
Department of Labour (Immigration New Zealand)	37	27
Government Communications Security Bureau	18	29
New Zealand Security Intelligence Service	10	15
Auckland District Health Board	10	9
TOTAL	287	263

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

TABLE 6: OUTCOMES FOR TOP RESPONDENT AGENCIES 2013/14

Agency	Closed	No interference with privacy	Complaint has some substance	Settled/ mediated	Referred to Director of Human Rights Proceedings
Department of Corrections	46	27	19	18	0
New Zealand Police	63	47	16	17	0
Ministry of Social Development	41	22	18	15	2
Accident Compensation Corporation	33	18	15	14	0
Department of Labour (Immigration New Zealand)	27	15	12	11	0
Government Communications Security Bureau	29	18	11	11	0
New Zealand Security Intelligence Service	15	8	7	7	0
Auckland District Health Board	9	4	5	5	0
	263				2

Satisfaction survey

Each year, we measure our complaints service through a satisfaction survey. This year we changed our survey process to an online survey. For this reporting period, our survey results are from October 2013.

Our motivation for changing to an online survey process was to encourage more customer feedback. For the nine months that we surveyed this year, we received 185 responses.

Participants were asked to rate the various factors by indicating whether they were very satisfied, satisfied, neither satisfied nor dissatisfied; dissatisfied or very dissatisfied.

We specifically asked complainants how easy or difficult it was to lodge a complaint. About 66% found it very easy or fairly easy and 19% found it neither easy nor difficult. Overall, 63% said they were satisfied with the overall quality of the service we provided, while 10% said they were neither satisfied or dissatisfied.

External audit

Again this year we contracted a barrister experienced in privacy issues to audit a random selection of 20 complaint files to determine the quality of the investigations process. The audit was undertaken with a focus on analysis of legal issues, clarity and sensitivity of communications and correspondence, fairness and timeliness of the process, and the efficiency of the complaint process.

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

The auditor commented that in attributing a score to a reviewed file a three indicated that the matter was handled adequately. A score of four indicated that the matter was handled professionally, accurately and efficiently. A score of five would be reserved for a matter that was dealt with in a way that demonstrated exceptional skill; something truly out of the ordinary and probably only attainable in a case that had thrown up a significant challenge to be overcome.

The audited files scored a total of 75.75. The average file score was 3.8. This is consistent with last year's audit.

Litigation

Most successful complaints are resolved during the course of our complaint investigation. There is always a small proportion of complaints where we find there has been an interference with privacy but where the parties do not settle. In some of those cases, litigation may be necessary or desirable, and we can refer the matter to the Director of Human Rights Proceedings.

This year, we referred 12 cases to the Director. This is a slight increase on last year (10). These added to the cases already with the Director for consideration.

During the year, the Director settled seven complaints, declined to take proceedings in seven, and filed proceedings in seven. The Director was considering whether to take proceedings in five remaining cases.

The Tribunal awarded compensation in both cases in which it found an interference with privacy (a total of $20,000 for two breaches in Geary v Accident Compensation Corporation, and $2,500 for failing to provide access in NOP and TUV v Chief Executive of MBIE).

Other litigation

The Court of Appeal refused leave for a litigant to appeal against the Employment Court's decision striking out a case against the Commissioner (among others): Aarts v Barnardos et al.

An application to bring defamation proceedings against us was struck out on the basis that the Commissioner has an absolute privilege in relation to statements that are made in the course of complaint investigations: Rafiq v Privacy Commissioner.

An application for judicial review was struck out: Murray v Commissioner of Police et al. The application repeated earlier unsuccessful proceedings against the Commissioner and other parties, and the Court of Appeal had already declared the proceedings an abuse of process earlier in the year.

We were granted leave to intervene in an appeal against a decision of the Tribunal to order discovery of confidential information to a litigant in an age discrimination case: Alpine Energy v Waters.

TABLE 7: REFERRALS, TRIBUNAL CASES AND OUTCOMES 2008-2014

	08/09	09/10	10/11	11/12	12/13	13/14
Referrals to Director	12	18	17	5	10	12
New proceedings in HRRT	29	13	25	21	10	22
Settled/withdrawn in HRRT	3	12	4	10	10	3
Costs awarded	4	2	6	0	3	4
Struck out	3	2	4	1	1	1
No interference	6	5	5	4	11	1
Interference	1	2	3	2	4	2

Breach notifications

We continued to receive a significant number of data breach notifications throughout the year. As the reporting requirement is voluntary, we are unable to qualify whether these figures represent a trend or the actuality of data breach within the broader business and government sectors.

Although the upward trend of breach reports (Table 8) is on its face cause for concern, we cannot tell whether those increases reflect an increase in actual incidence of breach. We are pleased that agencies are including reports to us as this gives us the opportunity to provide advice and to disseminate lessons about the causes of the breach so that other agencies can take steps to avoid similar occurrences.

The most common feature among the reported breaches is human error or carelessness. Nearly half of the reported data breaches involved physical information sent to the wrong entity or sent out in the wrong form, and a significant variety of email error events.

With the likelihood of mandatory reporting being within the statute in the foreseeable future we expect that reporting will increase as agencies come to understand their obligations to report incidents.

TABLE 8: NUMBERS OF NOTIFICATIONS AND SECTOR OF ORIGIN

Year	Total notifications	Public sector	Private sector
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
13/14	113	86	27

TABLE 9: MOST COMMON SECTORS FOR NOTIFICATIONS

Organisation type	08/09	09/10	10/11	11/12	12/13	13/14
Government	7	9	15	27	51	52
Hospital	5	1	3	5	12	10
Other health agencies	0	2	3	2	6	10
Large businesses (general)	1	0	3	3	7	6
Education sector	1	0	1	1	4	3
Small businesses	2	0	2	2	5	1
Local authorities	0	0	0	0	3	2
Banking/Finance/Insurance	0	0	3	3	4	8
Telecommunications	0	1	0	2	3	2

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	08/09	09/10	10/11	11/12	12/13	13/14
Website problem	3		2	2	12	6
Loss/theft of physical file	5	4	2	7	5	15
Loss/theft of portable storage device	1	3	1	5	7	1
Employee browsing	1		1	3	6	1
Electronic information sent to wrong recipient	2		2	10	17	27
Physical information sent to wrong recipient	2	3		5	23	23
Hacking			4	1	4	4

Policy

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

- providing advice to Cabinet and Parliament on the privacy implications of legislative proposals and other privacy initiatives
- providing 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:

- 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 effect on New Zealanders' privacy when they create new laws.

Assessing the quality of our advice

We assess the impact of our advice on whether we are able to achieve positive changes to policy directions. We are also continuing to try to reduce the number of instances where the Office is required to intervene by helping agencies to build their own capability. Agencies are now less likely to send us files with few or no privacy issues simply for our information, which may be a sign of greater confidence in their own judgment about privacy.

We assessed the impact of our advice on 41 policy files:

- 66% raised privacy issues that we considered needed further attention (up from 57% in 2012/13)
- 96% of files requiring further consideration saw some improvement as a result of our advice (up from 92% in 2012/13)
- 52% were "substantively improved" (up from 31% in 2012/13).[1]

This year saw continued improvement in our influence on government policy, with increases in both the proportion of files where we were able to get improvements, and how much improvement we were able to achieve. In last year's annual report, we suggested that government receptiveness to privacy had improved in the wake of several high-profile data breaches. This remains an important factor. Also, government and business agencies alike are realising that their focus should not purely be on security. Security is only one element of privacy protection. Other aspects of the information life cycle are equally important such as limiting what is collected, and deleting information once it is no longer needed.

We did a stakeholder survey during the year. It showed that the Office's opinion is taken seriously and that the Office is well-regarded.

Major legislative and policy projects the Office contributed to this year include:

- Continued support for government efforts to improve personal information management in the public sector, including by supporting the establishment of the Government Chief Privacy Officer
- Continued support for the Ministry of Justice on reform of the Privacy Act in response to the Law Commission's report
- Working with MBIE and making a submission on managing privacy risks arising for sole traders from the creation of a New Zealand Business Number
- Working with the New Zealand Data Futures Forum, including making a submission on its report
- Working with the Ministry of Justice and making a submission to the Social Services Committee select committee on the proposal to create Child Harm Prevention Orders within the Vulnerable Children Bill
- Advising Inland Revenue about the privacy impacts of the US Foreign Account Tax Compliance Act.

Health advice

Health information privacy is an important part of the Office's work, particularly as regional and national electronic health records become widespread. We receive some funding from the Ministry of Health under a memorandum of understanding, to support our capacity to provide advice. We have also advised agencies developing and operating electronic health records, with a focus on suggesting ways they can foster public and provider trust.

During the year, the Office has had an advisory position in the National Health IT Board's Health Information Governance Expert Advisory Group, which is working to develop a Health Information Governance Framework.

1. Note that figures for past years reflect revisions during the reporting year, and therefore may not be the same as those reported in the 2012/13 Annual Report.

Another major initiative during the year has been a review of three electronic health record initiatives to assess how successfully they deal with privacy issues. The resulting report provides recommendations for future providers of electronic health record services.

We have also maintained an active programme of awareness-raising through speaking engagements and articles on privacy issues targeted at the health sector.

Technology advice

The Office's efforts to improve privacy practice in the private sector are focused on supporting New Zealand business to better understand privacy risks and solutions in order to realise the benefits of new technology. We keep a close watch on new and developing technologies so that we are well placed to deliver helpful and timely advice.

This year, we undertook an assessment of the Law Commission's recommendation to produce a code of practice on biometrics. While we identified a number of privacy risks arising from the more widespread use of biometric technologies, our assessment was that a code could not be readily constructed to assist in managing these risks. We are therefore considering other options for managing the privacy issues arising from use of biometrics.

Also this year, we developed guidance for developers of mobile applications or "apps". Our *"Need to know or nice to have"* guidance was launched in July 2014.

Approved Information Sharing Agreements

In February 2013, Parliament passed the Privacy Amendment Act 2013. This Act amended the Privacy Act to allow government departments to share information in order to provide public services when the 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 requirements, and to seek reviews.

During the year, we were consulted on two information sharing agreements which progressed to completion:

- between Inland Revenue and the Department of Internal Affairs authorising the disclosure of passport information to Inland Revenue to enable it to make contact with overseas-based student loan borrowers and liable parents who are in default of their obligations.
- between Inland Revenue and New Zealand Police authorising the disclosure of information to Police in relation to serious crime.

The agreement between Inland Revenue and the Department of Internal Affairs was subsequently amended to allow for information to be shared on overseas-based student loan borrowers who are compliant with their obligations, consistent with changes to the Student Loans Act.

We were also consulted on a number of proposals including MSD Vulnerable Children initiatives and continue to work with officials.

Use of the information sharing provisions of the Act has been significantly lower than initially expected.

Agencies report some uncertainty about the processes that the legislation requires them to follow. This is something that we assist with and have begun to develop guidance on our role and expectations in relation to proposed sharing agreements. However, our statutory role precludes us from providing the "all of government" support required to give effect to this potentially powerful "all of government" tool. We are hopeful that some more central coordination will be available to assist agencies in the coming year.

Codes of Practice

At the start of the year, there were six codes of practice in force. No new codes were issued, but two amendments were proposed during the year and issued shortly after the year-end.

Justice Sector Unique Identifier Code

This code provides a partial exemption from the prohibition in information privacy principle 12(2) against two agencies using the same unique identifier to identify an individual. The code permits a justice sector agency to assign to an individual being processed through the justice system a unique identifier previously assigned by another justice sector agency. The code has been in place since 1998 and recognises the importance of the practice pre-dating the Privacy Act of assigning a number to individuals being processed through the justice system as they move between the investigative, prosecution and punishment stages of the justice system administered by different State authorities.

Late in the year, we publicly notified a proposal to amend the code to substitute a new definition of 'offence'. This was not a substantive change to the code but was needed to bring the code's definition into line with a new definition in the Criminal Procedure Act 2011. The deadline for public submissions on the proposal closed in June. The amendment was issued shortly after the end of the reporting year on 21 July 2014.

Credit Reporting Privacy Code

The Credit Reporting Privacy Code limits the charges that may be made for access by individuals to credit information held about them by credit reporters. The general rule is that no charge may be made for such access. However, the code permits a "reasonable charge" to be made where access is required within five working days. These limits on charging have been in place since the code was issued in 2004.

In March 2014, the Privacy Commissioner reported on the results of a completed inquiry into the charging practices of a major credit reporter, Veda Advantage. The Commissioner's concluded view was that Veda was making charges that substantially exceeded what was "reasonable". When it became apparent that the company did not intend to bring its charging practices into conformity with the Commissioner's view of what the code permitted, the Commissioner decided that the code should be amended to provide an explicit limit on what may be charged instead of the more elastic concept of reasonableness.

A proposed amendment limiting permitted charges to $10 was duly notified and public submissions were invited by 17 May. Having received and considered eight public submissions, the Commissioner issued Amendment No. 9 just after the end of the reporting year on 24 July 2014 with the new charging limits coming into force on 1 September 2014.

Consultations with the Ombudsman

The Ombudsman 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 23 (previous year 16) consultations from the Ombudsman and completed and closed 19.

As in previous years, the privacy interests that gave rise to the most consultations were those dealing with employment issues.

Own motion investigations

In addition to the own motion investigation undertaken into Veda's charging (see page 7), others included investigations into Profile Engine and EQC.

Profile Engine

Profile Engine is an online platform created by Profile Technology Ltd (a New Zealand company) originally as a back-end search engine for Facebook. Profile Engine lawfully acquired and now holds the user data of around 450 million individuals. In 2011, Profile Engine also launched a social networking platform independent of Facebook, using the Facebook user data it had earlier acquired.

As a result of a number of local and international enquiries from individuals whose profiles are included in Profile Engine's database, the Privacy Commissioner conducted an investigation into Profile Engine's process for deleting personal information on request.

The investigation concluded that the process is satisfactory, complies with the requirements of the Privacy Act, and should be followed by individuals seeking to delete their profiles. As a result of the Commissioner's investigation, Profile Engine made a number of changes to the process designed to make it clearer and simpler for individuals to use.

EQC

In 2013, the Chief Ombudsman and the Privacy Commissioner undertook a joint investigation on the Earthquake Commission's (EQC) handling of information requests in the aftermath of the Canterbury earthquakes. The report released in December 2013 – *Information fault lines: Accessing EQC information in Canterbury* – was carried out to establish how a lengthy backlog of information requests might be fixed as quickly and sustainably as possible.

Following the Canterbury earthquakes, accessing information held by EQC has been of primary significance to property owners faced with making important decisions about their homes and assets.

The Privacy Act and the Official Information Act (OIA) are powerful tools that provide individuals with rights of access to information. They impose mandatory standards on agencies such as EQC including a stipulation that requests for information must be responded to within 20 working days.

By early 2013, it was clear that EQC was routinely breaching this requirement to the extent that, by late May, it was advising requesters there would be a 6-7 month delay before it could respond to information requests.

The investigation took a detailed look at the information requests received by EQC.

Our investigation showed that EQC had failed to comply with its OIA and the Privacy Act obligations to provide information to requesters in a timely manner. In our view, this was principally the result of:

- an over-complicated and risk averse approach to responding to information requests; and
- a tendency to be reactive rather than proactive in the dissemination of claim-related information.

The increase in EQC work was sudden and unprecedented. We believed that an increase in request volume could have been anticipated, prepared for, and possibly prevented. We made 13 recommendations to EQC.

EQC accepted all of those recommendations and is taking steps to implement them. In addition, EQC is implementing a major "business improvement initiative".

Information fault lines: Accessing EQC information in Canterbury report is available on our website at www.privacy.org.nz.

4. OFFICE OF THE PRIVACY COMMISSIONER

Independence and competing interests

The Privacy Commissioner has wide ranging functions. He must have regard to the information privacy principles in the Privacy Act 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 take account of New Zealand's international obligations, and consider any general international guidelines that are relevant to improved protection of individual privacy.

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

Reporting

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

Staff

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

The Assistant Commissioner (Auckland) is responsible for codes of practice and international issues.

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

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

The Public Affairs Manager is responsible for the communications, media and external relations functions of the Office.

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

Contract staff are involved in accounting work for the Office.

Equal employment opportunities

The Office of the Privacy Commissioner promotes Equal Employment Opportunities (EEO) to ensure that its people capability practises are in line with its obligations as a good employer. We have an EEO policy that is integrated with the human resource programmes outlined in the Statement of Intent 2014 and that encourages active staff participation in all EEO matters. These are reviewed annually, together with polices on recruitment, employee development, harassment prevention and health and safety.

During the year, the main areas of focus have been:

- Developing talent with the Office regardless of gender, ethnicity, age or other demographic factor
- Integration of new work practices which promote or enhance work life balance amongst employees, including family friendly practices
- We maintain equitable gender-neutral remuneration policies which are tested against best industry practice
- The Commissioner continues to place a strong emphasis on fostering a diverse workplace and inclusive culture.

TABLE 11: WORKPLACE GENDER PROFILE 2013/14 (AS AT 30 JUNE 2014)

	Women		Men		Total
	Full-time	Part-time	Full-time	Part-time	
Commissioner			1		1
Senior managers	1	1	3		5
Team leaders/ Senior Advisers	2		4		6
Investigating officers	4		1		5
Administrative support	5	2			7
Advisers (Technology & Policy, Communications)			4		4
Enquiries officers	1		1		2
Total	**13**	**3**	**10**		**30**

TABLE 12: WORKPLACE ETHNIC PROFILE 2013/14 (AS AT 30 JUNE 2014)

	Māori		Pacific Peoples		Asian (incl. Sth Asian)		Other Ethnic Groups		Pakeha / European	
	Full-time	Part-time	Full-time	Part-time	Full-time	Part-time	Full-time	Part-time	Full-time	Part-time
Commissioner									1	
Senior managers									5	
Team leaders/ Senior Advisers									6	
Investigating officers			1		1				3	
Administrative support					1				5	2
Advisors (Technology & Policy, Communications)					1				3	
Enquiries officers									2	

We do not collect information on employees' age or disabilities. If a disability is bought to our attention, we would take steps to ensure that the employee has the necessary support to undertake their duties.

Recruitment policies including the advertisement, comply with the good employer expectations of the EEO Trust.

We have formal policies regarding, bullying, harassment and the provision of a safe and healthy workplace. There is an appointed harassment officer and staff have ready access to external support through our employee assistance programme.

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 challenges a number of privacy values:

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

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

- ensuring that individuals are aware of the programme (rule 1)
- limiting the disclosure and use of information (rule 4)
- limiting the retention of information (section 101 and rule 6)
- notifying individuals and allowing them time to challenge a decision before any action is taken against them (section 103).

One of the Commissioner's functions is to require government departments to 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 Commissioner's reports are included in Appendix B.

A detailed description of information matching and each active programme is on the Commissioner's website at www.privacy.org.nz.

The year in information matching

Information matching is an approach that allows agencies to share information in a well managed and controlled manner. Each information match is designed and implemented as a separate process. Information matches have generally been well managed.

This year we have asked agencies to look more closely at their destruction of data once it is no longer required for the match. Issues with destruction were reported for 14 matches. One of these issues has already been resolved and work is underway to resolve the others.

Other issues noted are a failure to implement encryption for an online transfer, and the use of a unique identifier in making the match in one programme.

The matches are usually operated by specialist technical staff and, as a result, there is a tendency for relatively weak governance oversight in the organisations.

Our oversight of information matching during the year included monitoring 56 active programmes.

Outreach

We published one Information Matching Bulletin. Copies are available at www.privacy.org.nz. We ran one information matching workshop in March 2014 for staff from DIA.

Changes in authorised and operating programmes

Parliament passed no new information matching authorisations during the year.

The following two new programmes went live:

- Customs/MSD Warrants to Arrest
- BDM(Births)/IR New-Borns Tax Number

Programme reports

A detailed description of each active programme, including recent results can be found on the Privacy Commissioner's website at www.privacy.org.nz. See Appendix B.

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. From time to time, we will actively seek more detailed evidence of compliance with particular rules.

We describe programmes' compliance in the following manner. 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.

6: FINANCIAL REPORT FOR THE YEAR ENDED 30 JUNE 2014

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 2014.

Privacy Commissioner

J Edwards

31 October 2014

General Manager

G F Bulog

31 October 2014

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 2014

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 45 to 67, that comprise the statement of financial position as at 30 June 2014, 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 35 to 45, that comprises the statement of service performance, and which includes outcomes.

Opinion

In our opinion:

- the financial statements of the Privacy Commissioner on pages 45 to 67:
  - comply with generally accepted accounting practice in New Zealand; and
  - fairly reflect the Privacy Commissioner's:
    - financial position as at 30 June 2014; and
    - financial performance and cash flows for the year ended on that date;
- the non-financial performance information of the Privacy Commissioner on pages 35 to 45:
  - complies with generally accepted accounting practice in New Zealand; and
  - fairly reflects the Privacy Commissioner's service performance and outcomes for the year ended 30 June 2014, 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 31 October 2014. 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.

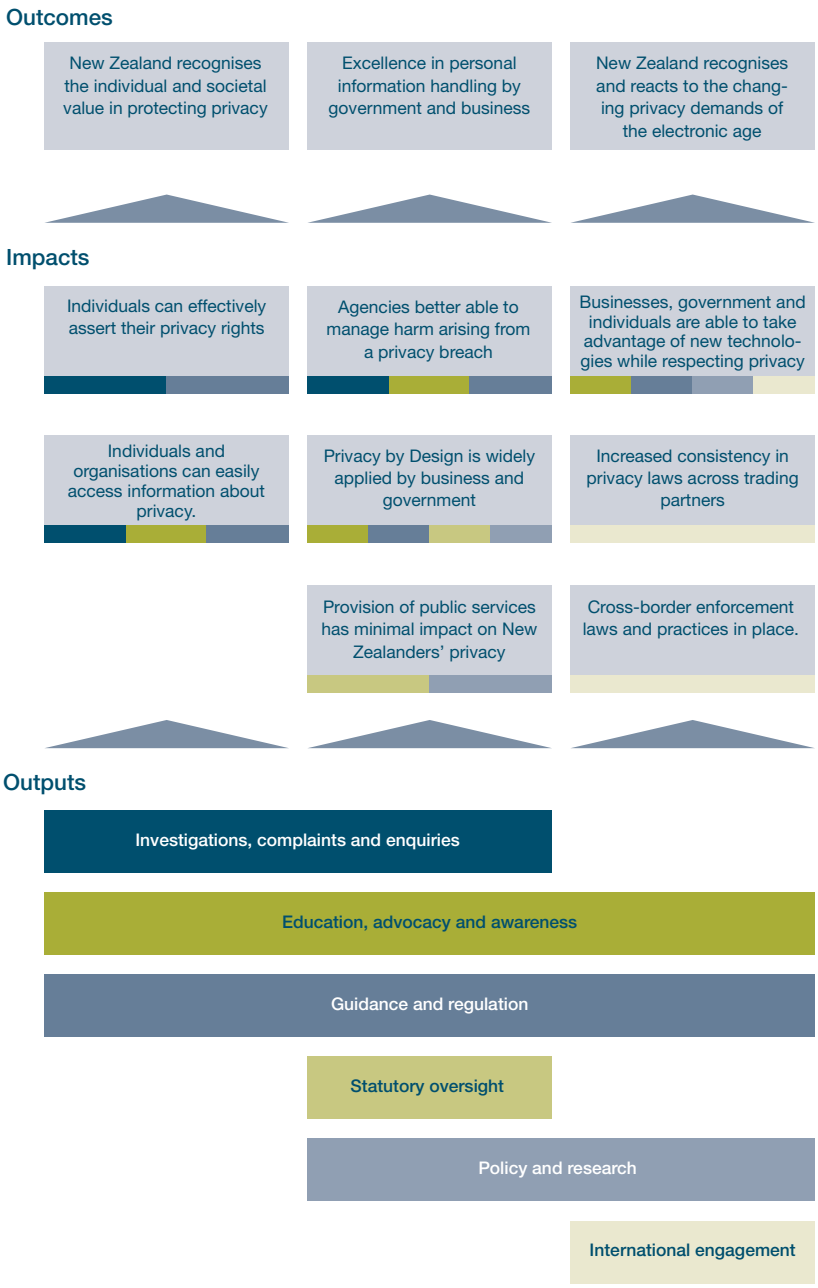
Leon Pieterse
Audit New Zealand
On behalf of the Auditor-General
Auckland, New Zealand

STATEMENT OF OBJECTIVES AND SERVICE PERFORMANCE 2013/14

The Office of the Privacy Commissioner is an Independent Crown entity and strongly maintains such independence. The work programme complements government priorities of growing the economy and improving the quality and responsiveness of public services.

A set of performance measures has been developed 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 our resources. The outcomes framework links those outcomes contained within the mission statement of the Privacy Commissioner with inputs supported by measurable service performance standards.



GOVERNANCE AND ACCOUNTABILITY

The Privacy Commissioner is a corporation sole. With the appointment of a new Privacy Commissioner, an independent review of governance and accountability was undertaken.

The objectives of the review were to:

a) brief the Commissioner on the Office's governance environment and systems (both internal and external), its internal management systems, and its approach to meeting its statutory accountability obligations;
b) identify areas where the Office's systems and practices could be improved, and make recommendations for how they could be improved; and
c) provide information to assist the Commissioner and the senior leadership team in meeting the Office's planning and reporting obligations under the Crown Entities Act 2004.

The overall conclusions from the review were:

1) the Office appears to be fundamentally sound. It has strong corporate capability, good policies and practices, and no obvious financial risks;
2) external relationships appear to be good, and from those I spoke to there is confidence in the Office's ability to perform effectively as a Crown entity and to meet its accountability obligations;
3) the Office is also well placed to meet the challenges of the new planning and reporting environment. But it will need to devote time and resources to do so effectively.

The key issues and challenges facing the Office in governance and accountability terms were identified as being:

a) the need to develop a governance doctrine for the Office, and improve the focus on the respective roles of board oversight and management;
b) the reliance on a limited number of individuals for its corporate and financial management and broader institutional knowledge, and the need for succession planning;
c) the lack of an active risk management focus or culture;
d) the need to enhance the Office's policies and systems on conflict of interest management;
e) in respect of planning and reporting, the need to respond effectively to Audit New Zealand's recommendations about the quality of its performance measures and the need to link those measures to its business systems; and
f) the need for ongoing vigilance about the Commissioner's independence, especially in relation to the Better Public Services reforms and the process of setting annual Ministerial "expectations".

ACTIONS TAKEN

The key issues identified in the review have been actioned either to completion or near completion by 30 June 2014.

In June 2014 the Commissioner established a Governance Advisory Board (GAB). The purpose of the GAB is to provide the Privacy Commissioner with advice and guidance on the principles of governance in relation to the discharge of his functions under the Crown Entities Act and on other issues that may arise.

The GAB are not involved in any way with setting the work programme or management of the Office and do not have any knowledge of or involvement in, any complaints received by the Privacy Commissioner. Further, the GAB do not comment on the operational aspects of the senior leadership team's responsibilities.

The GAB reflects we are a small Crown entity. Governance oversight needed a proportionate group who could reasonably be expected to provide an appropriate level of advice and guidance.

The members of the GAB are:

- John Edwards, Privacy Commissioner
- Robert Buchanan, Public law and governance practitioner
- Judith Johnston, Management consultant

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	3,584
Other Revenue	300	329
Total Revenue	3,548	3,913

The Privacy Commissioner received additional funding of $336,000 on 20 June 2014, as approved by Cabinet on 14 April 2014 and included in the Supplementary Estimates of Appropriations for the Government of New Zealand for the year ending 30 June 2014.

STATEMENT OF OBJECTIVES AND SERVICE PERFORMANCE

FOR THE YEAR ENDED 30 JUNE 2014

	Actual 2014 $000	Budget 2014 $000	Actual 2013 $000
OUTPUT 1:			
Investigations, complaints and enquiries			
Resources employed			
Revenue	1,206	1,092	1,556
Expenditure	1,218	1,097	1,509
Net Surplus(Deficit)	(12)	(5)	47
OUTPUT 2:			
Education, advocacy and awareness			
Resources employed			
Revenue	795	721	1,384
Expenditure	803	724	1,334
Net Surplus(Deficit)	(8)	(3)	50
OUTPUT 3:			
Guidance and regulation			
Resources employed			
Revenue	409	371	704
Expenditure	414	373	665
Net Surplus(Deficit)	(5)	(2)	39

	Actual 2014 $000	Budget 2014 $000	Actual 2013 $000
OUTPUT 4:			
Statutory oversight			
Resources employed			
Revenue	371	336	704
Expenditure	374	337	665
Net Surplus(Deficit)	(3)	(1)	39
OUTPUT 5:			
Policy and Research			
Resources employed			
Revenue	698	633	704
Expenditure	706	636	665
Net Surplus(Deficit)	(8)	(3)	39
OUTPUT 6:			
International			
Resources employed			
Revenue	434	394	704
Expenditure	434	396	665
Net Surplus(Deficit)	-	(2)	39
TOTALS:			
Resources employed			
Revenue	3,913	3,548	3,644
Expenditure	3,949	3,563	3,508
Net Surplus(Deficit)	(36)	(15)	136

OUTCOME 1: NEW ZEALANDERS RECOGNISE THE INDIVIDUAL AND SOCIETAL VALUE IN PROTECTING PRIVACY

Why is this important?

Privacy is best protected when a society consistently attaches value to it as a right, and works to ensure that it is respected. Achieving this end requires both that individuals are able to effectively assert their rights and obtain redress when those rights have been compromised, and that organisations and individuals have the information they need to recognise and protect those rights through their activities.

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 can effectively assert their privacy rights
- Individuals and organisations can easily access information about privacy

OUTPUT MEASURES

Investigations, complaints and enquiries

Quantity			
Measure	Estimate	Achieved 2013/14	Achieved 2012/13
Estimated number of enquiries received and answered	5,000–7,000	8,765	9,038
Number of complaints received	800–1,000	Not achieved 725 received	824
Number of current complaints processed to completion or settled or discontinued	800–1,000	Not achieved 702 processed	896

The number of complaints received has reduced in 2013/14 from the previous year due to the significant impact in that year of some high profile data breaches including the ACC and MSD breach in 2012 and the later breach in 2013 breach by the Earthquake Commission.

Closure of complaints was impacted by the absence of trained staff due to parental leave and staff turnover during the year which reduced the number of staff available to undertake the complaint investigations.

Quality		
Measure	**Estimate**	**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	80%	Not achieved (2012/13 Not achieved 70%) 60% of complainants' and respondents' satisfaction with the complaints handling process was rated as "satisfactory" or better. 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. 39% of complainants and 87% of respondents rated the process as satisfactory or better. Though the measure is satisfaction with the process it is anticipated that satisfaction for complainants is affected 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 2014. Improvements to the format and collection methods provide for improved reporting compared to previous years.
Of the complaints processed, 30% are closed by settlement between the parties	30%	Achieved 32% (2012/13 Achieved 36%) 32% of complaints were closed by settlement between the parties.
In 80% of the complaints closed we demonstrate personal contact, either by phone or in person, with one or more of the parties	80%	Not achieved 67% (2012/13 Not achieved 69%) 67% of complaints closed demonstrated personal contact, 2% down on the previous year. We continue to strive to meet the ambitious target of 80%. The investigations team is a small team and with a staff member on parental leave through the period, staff turnover and the need to use trained staff on other projects impacted on the flexibility of our investigators to meet the higher target of 80% and maintain closure rates in line with service standards for timeliness.
An external review of a sample of complaints investigations rates 70% as 4 out of 5 or better on the legal analysis, correctness of the legal conclusions, soundness of the investigative procedure and timeliness of response	70%	Not achieved (new measure) 29% of the sample were rated 4 out of 5 or better. The average rating was 3.78 only marginally below the performance standard with 91% rating 3.75 or better. As a new measure, the subjective nature of the marking may better be reflected in performance as an average rating, rather than a percentage.

Timeliness		
Measure	Estimate	Achievement
80% of complaints are completed, settled or discontinued within nine months of receipt	80%	Achieved (2012/13 Achieved 93%) 88% of complaints were completed, settled or discontinued.
Respond to 90% of 0800 line enquiries within one working day	90%	Achieved (2012/13 Achieved 94%) 94% of enquiries were responded to within one working day.
Respond to 70% of phone enquiries live	70%	Achieved (2012/13 Not achieved 66%) 99% of phone enquiries were responded to live.

OUTCOME 2: 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 by no means universal. Poor information handling practices by government and business is a 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 adverse impact on New Zealanders' privacy.

OUTPUT MEASURES

Education, advocacy and awareness

Quantity			
Measure	Estimate	Achieved 2013/14	Achieved 2012/13
Education workshops delivered	30–40	39	36
Presentations at conferences / seminars	30–40	62	70
Media enquiries received	250–300	286	310
Comprehensive privacy website maintained	Achieved	Achieved (new measure) The website is regularly updated. Significant additional features have been included such as a blog facility and enhanced analytics.	

Quality		
Measure	**Estimate**	**Achievement**
Evaluations show that the expectations of 90% of attendees at workshops were either met or exceeded for quality of presentations	90%	Achieved 89% (2012/13 Achieved 99%) The overall percentage achieved is calculated across a range of quality measures with attendees rating each measure. 93% of attendees who completed the evaluation agreed or strongly agreed that they would recommend the workshop to others. 90% agreed or strongly agreed that the presenters communicated their material effectively, and 94% said that the materials were of a high standard. Evaluations are now web based resulting in improved response rates.
Website contains up-to-date copies of all privacy codes and commentary, all formal statutory reports of the Privacy Commissioner, all current published guidance from the Office, and additional resources to support compliance with the Privacy Act	Achieved	Achieved (new measure)

Timeliness		
Measure	**Estimate**	**Achievement**
90% of media enquiries are recorded, and responded to if required within agreed deadlines	Achieved	Achieved 100% (New measure)

GUIDANCE AND REGULATION

Quantity		
Measure	**Estimate**	**Achievement**
Major pieces of guidance produced	1	Achieved 1 (new measure) The Office produced guidance materials for mobile application developers and published on our website.
Reviews or updates of Codes published	2	Not applicable (new measure) Reviews and updates of codes are demand driven by affected sectors. Two code amendments were commenced in 2013/14 but their completion is 2014/15.

Quantity		
Measure	Estimate	Achievement
Qualitative evaluation or review of major pieces of guidance	1	Not achieved (new measure) Premised on additional funding being available during the financial year. The additional funding did not become available until June 2014.
Amendments to codes of practice meet all statutory requirements	100%	Not applicable. No amendments to Codes were issued in 2013/14. (2012/13 Achieved 100%)

STATUTORY OVERSIGHT

Quantity		
Measure	Estimate	Achievement
Information matching programmes monitored	52	Achieved 56 (2012/13 Achieved 54)
New information sharing or matching programmes assessed	5–20	Not applicable (new measure) Dependent upon external agencies seeking to establish new programmes. Three new programmes were received despite estimates of significantly higher numbers being indicated by the agencies involved.
International information sharing agreements reviewed	4–8	Achieved (new measure) 6 international information sharing agreements were reviewed. The agreements were: Customs with Japan Customs with France Customs with the EU Immigration Five Country Conference (FCC) War Crimes MoU Immigration FCC MoU with USA Immigration with Indonesia.
Applications under other statutory consultation responsibilities	10–20	Achieved (new measure) 12 applications were reviewed Vehicle Register (10) Births Deaths and Marriages Act (2)

Quality		
Measure	Estimate	Achievement
All statutory obligations to report on information matching met	100%	Not applicable (new measure) Four information matches were commenced in 2013/14. They remain under progress for completion and reporting in 2014/15.

Timeliness		
Measure	**Estimate**	**Achievement**
Statutory timelines for reporting on information matching met	100%	Achieved (new measure) Four information matches were commenced in 2013/14. As required, they remain under progress.
Percentage of responses to requests to review information sharing agreements provided within agreed timeframes	90%	Achieved 100% (new measure)
Percentage of responses to requests to review international information sharing agreements provided within agreed timeframes	95%	Achieved 100% (new measure)

POLICY AND RESEARCH

Quantity		
Measure	**Estimate**	**Achievement**
New policy files opened during the year	60–100	Achieved (new measure) 81 new policy files were opened and actioned.

Quality		
Measure	**Estimate**	**Achievement**
Independent assessment of a representative sample of advice provided on policy files rates 70% as 4 out of 5 or better	70%	Achieved (new measure) The sample consisted of seven major pieces of policy comprising about 450 documents in total. The independent assessor gave an overall rating for the sample as excellent in terms of the quality of analysis, focus on important issues, clear communications and good working relationships with counterparts.

Timeliness		
Measure	**Estimate**	**Achievement**
Advice on proposals provided within agreed timeframes	90%	Not achieved (new measure) 84% of advice on proposals presented were provided within agreed timeframes.

OUTCOME 3: NEW ZEALANDERS RECOGNISE AND REACT TO THE CHANGING PRIVACY DEMANDS OF THE ELECTRONIC AGE

Why is this important?

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

Often new technologies and applications are developed and put into use before analysing privacy implications. Existing regulatory frameworks were not established with the IT revolution 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 Office of the Privacy Commissioner in its 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 the appropriate response.

A distinct feature of the emerging digital environment is the globalisation of information flows and information collection via the internet. International cooperation has become essential to protecting New Zealanders' privacy effectively. Conversely, New Zealand businesses' own ability to engage in the global information economy relies on a regulatory regime and approach that are consistent with those in other countries.

The impacts we seek

- Businesses, government and individuals are able to take advantage of new technologies while respecting privacy.
- The Privacy Act is recognised as meeting the requirements of our trading partners.
- Cross-border enforcement laws and practices are in place.

OUTPUT MEASURES

International

Quantity		
Measure	**Estimate**	**Achievement**
International forums engaged in	4	Achieved 8 (2012/13 Achieved 4) Eight International forums were engaged in by the Commissioner or representatives of the Privacy Commissioner. Provided a delegate to each of the APPA forums (three meetings). Various international data protection conferences and workshops, including presentation of papers and chair of sessions.

Quality		
Measure	**Estimate**	**Achievement**
Our goals are progressed by international forums	Achieved	Achieved (new measure) Maintained recognition of New Zealand law meeting adequate level of data protection within the European Commission. New Zealand is a participant in APEC CPEA and GPEN and the office is represented on the governance committees of both enforcement networks.
Our participation in forums is valued by partners	Achieved	Achieved (2012/13 Achieved) Continued in role on governance committees of CPEA and GPEN. Continued to receive invitations to speak at international events.

STATEMENT OF ACCOUNTING POLICIES

FOR THE YEAR ENDED 30 JUNE 2014

Reporting entity

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

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

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

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

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

The financial statements for the Privacy Commissioner are for the year ended 30 June 2014, and were approved by the Commissioner on 31 October 2014. The financial statements cannot be altered after they have been authorised for issue.

Basis of preparation

Statement of Compliance

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

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

Measurement base

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

Functional and presentation currency

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

Significant Accounting policies

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

Budget figures

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

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

Additional funding of $336,000 was approved by Cabinet on 14 April 2014 and included in the Supplementary Estimates of Appropriations for the Government of New Zealand for the Year Ending 30 June 2014. The additional funding was not included in budget figures.

Revenue

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

Revenue from the Crown

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

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

Other grants

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

Interest

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

Sale of publications

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

Rental Income

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

Provision of services

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

Funded Travel

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

Leases

Operating leases

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

Goods and Services Tax (GST)

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

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

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

Commitments and contingencies are disclosed exclusive of GST.

Income Tax

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

Cash and cash equivalents

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

Debtors and other receivables

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

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

Inventories

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

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

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

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

Property, plant and equipment

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

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

Revaluations

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

Depreciation

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

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

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

Additions

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

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

Disposals

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

Subsequent costs

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

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

Intangible assets

Software acquisition

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

Staff training costs are recognised as an expense when incurred.

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

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

Amortisation

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

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

Acquired computer software	4 years	25%

Impairment of non-financial assets

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

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

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

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

Creditors and other payables

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

Employee Entitlements

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

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

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

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

Superannuation schemes

Defined contribution schemes

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

Financial instruments

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

Statement of cash flows

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

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

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

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

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

Critical accounting estimates and assumptions

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

Property, plant and equipment useful lives and residual value

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

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

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

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

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

Critical judgements in applying the Privacy Commissioner's accounting policies

Management has exercised the following critical judgements in applying the Privacy Commissioner's accounting policies for the period ended 30 June 2014:

Leases classification

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

Non-government grants

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

Changes in accounting policies

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

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

- Amendments to NZ IAS 1 Presentation of Financial Statements. The amendments introduce a requirement to present, either in the statement of changes in equity or the notes, for each component of equity, an analysis of other comprehensive income by item. The Privacy Commissioner, would present this analysis in note 6.
- FRS-44 *New Zealand Additional Disclosures and Amendments to NZ IFRS to harmonise with IFRS and Australian Accounting Standards (Harmonisation Amendments)* – The purpose of the new standard and amendments is to harmonise Australian and New Zealand accounting standards with source IFRS and to eliminate many of the differences between the accounting standards in each jurisdiction. 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:

- NZ IFRS 9 Financial Instruments will eventually replace NZ IAS 39 Financial Instruments: Recognition and Measurement. NZ IAS 39 is being replaced through the following 3 main phases: Phase 1 Classification and Measurement, Phase 2 Impairment Methodology, and Phase 3 Hedge Accounting. Phase 1 has been completed and has been published in the new financial instrument standards NZ IFRS 9. NZ IFRS 9 uses a single approach to determine whether a financial asset is measured at amortised cost or fair value, replacing the many different rules in NZ IAS 39. The approach in NZ IFRS 9 is based on how an entity manages its financial assets (its business model) and the contractual cash flow characteristics of the financial assets. The financial liability requirements are the same as those of NZ IAS 39, except for when an entity elects to designate a financial liability at fair value through the surplus/deficit. The new standard is required to be adopted for the year ended 30 June 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 for 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 NZ IFRS and amendments to existing NZ IFRS will not be applicable to public benefit entities. Therefore, the XRB has effectively frozen the financial reporting requirements for public benefit entities up until the new Accounting Standard Framework is effective. Accordingly, no disclosure has been made about new or amended NZ IFRS that exclude public benefit entities from their scope.

STATEMENT OF COMPREHENSIVE INCOME

FOR THE YEAR ENDED 30 JUNE 2014

	Note	Actual 2014 $000	Budget 2014 $000	Actual 2013 $000
Revenue				
Crown Revenue	2	3,584	3,248	3,248
Other Revenue	3	297	260	361
Interest		32	39	34
Total Income		3,913	3,547	3,643
Expenditure				
Promotion	4	111	52	57
Audit Fees		27	20	27
Depreciation and Amortisation	1, 10, 11	100	150	142
Rental Expense		352	420	395
Operating Expenses		451	420	370
Staff Expenses	5	2,908	2,500	2,517
Total Expenditure		3,949	3,562	3,508
Surplus/(Deficit)		(36)	(15)	136
Other comprehensive income		-	-	-
Total Comprehensive Income		**(36)**	**(15)**	**136**

STATEMENT OF CHANGES IN EQUITY

FOR THE YEAR ENDED 30 JUNE 2014

	Note	Actual 2014 $000	Budget 2014 $000	Actual 2013 $000
Total Equity at the start of the year	1	792	418	656
Operating surplus for the period		-36	-15	136
Total recognised revenue and expenses for the period		-36	-15	136
Total Equity at the end of the year	**6**	**756**	**404**	**792**

Explanations of major variances are provided in Note 1

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

STATEMENT OF FINANCIAL POSITION

AS AT 30 JUNE 2014

	Note	Actual 2014 $000	Budget 2014 $000	Actual 2013 $000
Public Equity				
General funds	6	756	403	792
Total public equity		756	403	792
Current assets				
Cash & cash equivalents	7	798	367	696
Debtors and other receivables	8	2	75	34
Inventory	9	11	8	8
Prepayments	8	22	4	15
Total Current Assets		833	454	753
Non-current assets				
Property, Plant & Equipment	10	149	161	199
Intangible assets	11	64	0	52
Total non-current assets		213	161	251
Total assets		**1,046**	**615**	**1,004**
Current liabilities				
Creditors and other payables	12	167	131	103
Employee entitlements	13	122	80	109
Total current liabilities		289	211	212
Total Liabilities		289	211	212
Net assets		**756**	**404**	**792**

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

STATEMENT OF CASH FLOWS

FOR THE YEAR ENDED 30 JUNE 2014

	Note	Actual 2014 $000	Budget 2014 $000	Actual 2013 $000
Cash flows from operating activities				
Cash was provided from:				
Supply of outputs to the Crown		3,790	3,248	3,454
Revenues from services provided		96	260	150
Interest received		32	40	34
Cash was applied to:				
Payment to suppliers		904	913	835
Payments to employees		2,895	2,500	2,535
Net Goods and Services tax		(44)	14	11
Net cash flows from operating activities	14	163	121	257
Cash flows from investing activities				-
Cash was applied to:				
Purchase of Property Plant and Equipment		27	110	30
Purchase of Intangible Assets		34	-	-
Net cash flows from investing activities				
Net increase (decrease) in cash held		102	(15)	227
Plus opening cash		696	357	468
Closing cash balance		798	342	696
Cash and bank		798	367	696
Closing cash balance		**798**	**367**	**696**

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

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

NOTES TO THE FINANCIAL STATEMENTS

FOR THE YEAR ENDED 30 JUNE 2014

NOTE 1: TOTAL COMPREHENSIVE INCOME

	Actual 2014 $000	Actual 2013 $000
The total comprehensive income is after charging for:		
Fees paid to auditors		
External audit	-	-
Current year	27	27
Prior year	27	24
Depreciation:		
Furniture & fittings	17	78
Computer equipment	54	57
Office equipment	7	7
Total depreciation for the year	78	142
Amortisation of intangibles	22	
Rental expense on operating leases	352	395

Explanation of major variances

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

Statement of Comprehensive Income

Additional funding of $336,000 was approved by Cabinet on 14 April 2014 and included in the Supplementary Estimates of Appropriations for the Government of New Zealand for the Year Ending 30 June 2014. The additional funding was received on 20 June 2014.

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 2014.

Rental Expenses

Rental expenses were lower than budget due to the signing of a new lease for the Auckland office which included a six month rent free period.

Promotion expenses

The necessity to produce updated guidance materials, education materials for schools and other initiatives were funded from retained earnings to meet unbudgeted expenditure in this area.

The Office hosted the APEC and APPA conference in June 2013, a combined cost of $40,000.

Operating expenses

Increased expenditure in computer maintenance (including the replacement of computers as they came out of warranty) higher costs for domestic travel and subscription costs were major drivers of higher than budgeted expenditure on operating expenses.

Staff expenses

A new senior staff appointment was made in September 2013 as necessary support through the pending legislative change process and to provide necessary support to the delivery of services. The position was not included in the budget.

As part of her employment conditions as determined by the Remuneration Authority, the Privacy Commissioner was entitled to a retirement leave payment of $128,496 at the cessation of her term as Privacy Commissioner. A sum of $52,912 was received by this office from the Department of Prime Minister and Cabinet to reflect the portion of retirement leave attributable to earlier service with that Department.

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 (2013: $Nil).

NOTE 3: OTHER REVENUE

	Actual 2014 $000	Actual 2013 $000
Other grants received	206	206
Rental income from property sub-leases	25	25
Privacy Forum	25	22
Seminars & Workshops	38	43
Other	2	67
Total other revenue	**296**	**363**

NOTE 4: PROMOTION EXPENSES

	Actual 2014 $000	Actual 2013 $000
Website development expenses	41	20
Publications	2	4
Inventories consumed	-	-
Privacy Forum	8	10
Other marketing expenses	60	23
Total marketing expenses	**111**	**57**

NOTE 5: STAFF EXPENSES

	Actual 2014 $000	Actual 2013 $000
Salaries and wages	2,732	2,334
Employer contributions to defined contribution plans	34	76
Other Staff expenses	33	27
Other contracted services	99	96
Increase/(decrease) in employee entitlements	10	(16)
Total Staff Expenses	**2,908**	**2,517**

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 2014 $000	Actual 2013 $000
Opening balance	792	656
Net (deficit) / surplus	(36)	136
Closing balance	**756**	**792**

NOTE 7: CASH AND CASH EQUIVALENTS

	Actual 2014 $000	Actual 2013 $000
Cash on hand and at bank	51	31
Cash equivalents – on call account	747	665
Total cash and cash equivalents	**798**	**696**

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 2014 $000	Actual 2013 $000
Trade debtors	2	33
Prepayments	22	15
Total	**24**	**48**

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 (2013: $NIL).

Impairment

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

Aging analysis:	2014 $000	2013 $000
Not past due		
Past due 1-30 days	2	7
Past due 31-60 days	0	0.05
Past due 61-90 days	0.5	1
Past due >91 days	0	0.2
Total debtors and other receivables	2	8

As at 30 June 2014 no debtors have been identified as insolvent. (2013:$NIL).

NOTE 9: INVENTORIES

	Actual 2014 $000	Actual 2013 $000
Publications held for sale	11	8

The carrying amount of inventories held for distribution that are measured at current replacement cost as at 30 June 2014 amounted to $NIL (2013: $NIL).

There have been no write-down of inventories held for distribution or reversals of write-downs (2013 $NIL).

No inventories are pledged as security for liabilities (2013: $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 2012	415	289	95	799
Additions	0	12	6	18
Disposals	0	(53)	(30)	(83)
Balance at 30 June 2013	415	248	71	734
Balance at 1 July 2013	415	248	71	734
Additions	1	10	17	28
Disposals				
Balance at 30 June 2014	**416**	**258**	**88**	**762**
Accumulated depreciation and impairment losses				
Balance at 1 July 2012	**311**	**111**	**71**	**493**
Depreciation expense	60	57	7	124
Disposals		(53)	(30)	(83)
Balance at 30 June 2013	371	116	47	534
Balance at 1 July 2013	371	116	47	534
Depreciation expense	17	54	7	78
Elimination on disposal				
Balance at 30 June 2014	**388**	**170**	**54**	**612**
Carrying amounts				
At 1 July 2013	43	132	24	199
At 30 June 2014	**28**	**88**	**34**	**150**

NOTE 11: INTANGIBLE ASSETS

Movements for each class of intangible asset are as follows:

	Acquired software 2014 $000
Cost	
Balance at 1 July 2012	283
Additions	(210)
Balance at 30 June 2013	73
Balance at 1 July 2013	73
Additions	33
Balance at 30 June 2014	106
Accumulated amortisation and impairment losses	
Balance at 1 July 2012	281
Amortisation expense	(260)
Balance at 30 June 2013	21
Balance at 1 July 2013	21
Amortisation expense	21
Balance at 30 June 2014	42
Carrying amounts	
At 1 July 2012	2
At 30 June and 1 July 2013	52
At 30 June 2014	64

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 2014 $000	Actual 2013 $000
Creditors	73	34
Accrued expenses	76	68
Other payables	18	-
Total creditors and other payables	**167**	**103**

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 2014 $000	Actual 2013 $000
Current employee entitlements are represented by:		
Accrued salaries and wages	13	-
Annual leave	109	109
Total current portion	122	109
Current	122	109
Non-current	-	-
Total employee entitlements	**122**	**109**

NOTE 14: RECONCILIATION OF TOTAL COMPREHENSIVE INCOME FROM OPERATIONS WITH THE NET CASHFLOWS FROM OPERATING ACTIVITIES

	Actual 2014 $000	Actual 2013 $000
Total comprehensive income	(36)	136
Add/(less) non-cash items:		
Depreciation and Amortisation	100	142
Other non-Cash Items	-	-
Total non-cash items	**100**	**142**
Add/(less) movements in working capital items:		
Increase/(Decrease) in creditors	39	(12)
Increase/(Decrease) in accruals	7	8
(Increase)/Decrease in inventory	(3)	3
Increase/(Decrease) in payables	37	3
Increase/(Decrease) in employee entitlements	13	(18)
Increase/(Decrease) in Income in Advance	-	-
(Increase)/Decrease in receivables	6	(5)
Working capital movements - net	**99**	**(21)**
Add/(less) items classified as investing activities:	-	-
Landlord's capital contribution	-	-
Net cash flow from operating activities	**163**	**257**

NOTE 15: CAPITAL COMMITMENTS AND OPERATING LEASES

Capital commitments

The Privacy Commissioner has capital commitments of $47,050 for the completion of the telecommunications upgrade for the year 2013/14. (2013: $nil)

Operating leases

	Actual 2014 $000	Actual 2013 $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	345	295
Later than one year and not later than five years	614	833
Later than five years	11	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 on the Auckland premises expire 31 July 2019. The sub tenant can give 6 months' notice to terminate their lease agreement.

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 (2013: $14,427). 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 (2013: $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 Privacy Commissioner as well as being its major source of revenue.

Marie Shroff (Privacy Commissioner) was a Board Member of the Equal Employment Opportunities Trust. The Office paid the Trust $200 for membership fees. There were no other transactions with this Trust during the current financial year. (In 2013 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 2014 $000	Actual 2013 $000
Total salaries and other short-term employee benefits	1,123	883

Key management personnel include all senior managers and the Privacy Commissioner who together comprises the Senior Leadership Team (SLT). An additional member joined the SLT in April 2014 The actual 2014 figure includes the one-off retirement leave payment made in accordance with the employment provisions of the Privacy Commissioner at the cessation of her term (Refer to Note 1: Explanation of major variances) and a $10,000 acting up payment to an SLT member.

NOTE 18: EMPLOYEES' REMUNERATION

The Office of the Privacy Commissioner is a Crown Entity and is required to disclose certain remuneration information in its 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 2014	Actual 2013
$100,000 - $109,999		1
$110,000 - $119,999	2	-
$120,000 - $129,999		-
$130,000 - $139,999		-
$140,000 - $149,999	1	2
$150,000 - $159,999	2	1
$160,000 - $169,999		1
$170,000 - $179,999	1	-
$280,000 - $289,999		1

NOTE 19: COMMISSIONERS' TOTAL REMUNERATION

In accordance with the disclosure requirements of Section 152 (1)(a) of the Crown Entities Act 2004, the total remuneration includes all benefits paid during the period 1 July 2011 to 30 June 2014. John Edwards was appointed Privacy Commissioner to replace Marie Shroff effective on 17 February 2014

Name	Position	Amount 2014	Amount 2013
Marie Shroff	Privacy Commissioner (1 July 2013 to 16 February 2014)	$287,812	$284,177 (Full year)
John Edwards	Privacy Commissioner (From 17 February 2014)	$102,783	Nil

The amount paid to Marie Shroff includes retirement leave due in accordance with her employment provisions, at the cessation of her term as Privacy Commissioner. (Refer to Note 1: Explanation of major variances)

NOTE 20: CESSATION PAYMENTS

No redundancy payments were made in the year. (2013: $Nil)

NOTE 21: INDEMNITY INSURANCE

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

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

23A Financial instrument categories

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

	2014 $000	2013 $000
FINANCIAL ASSETS		
Loans and Receivables		
Cash and cash equivalents	798	696
Debtors and other receivables	2	34
Total loans and receivables	800	730
FINANCIAL LIABILITIES		
Financial liabilities at amortised cost		
Creditors and other payables	167	103
Total financial liabilities at amortised cost	**167**	**103**

23B 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 2014 (2013: $Nil). The Privacy Commissioner has no exposure to interest rate risk.

Liquidity risk

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

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

Market risk

Fair value interest rate risk

The Privacy Commissioner's exposure to fair value interest rate risk is limited to its bank deposits which are held at fixed rates of interest. The Privacy Commissioner does not hold significant interest-bearing assets, and have no interest-bearing liabilities. The Privacy Commissioner invests cash and cash equivalents with the ANZ Bank, ensuring a fair market return on any cash position, but do not seek to speculate on interest returns, and do not specifically monitor exposure to interest rate returns.

Cash flow interest rate risk

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

Interest rate exposure – maturity profile of financial instruments

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

	Weighted average effective interest rate	Variable interest rate	Fixed maturity dates – less than 1 year	Non-interest bearing
2014	%	NZ$000	NZ$000	NZ$000
Financial assets				
Cash and cash equivalents		798		
		798		
2013				
Financial Assets				
Cash and cash equivalents		696		
		696		

Interest rate sensitivity

The sensitivity (percentage movement) analysis in the table below of the effect on net surplus has been determined based on the exposure to interest rates at the reporting date and the stipulated change taking place at the beginning of the financial year and held constant throughout the reporting period. A 100 basis point change is used when reporting interest rate risk internally to the Commissioner and represents Privacy Commissioner's assessment of a reasonably possible change in interest rates.

	Net surplus 2014 NZ$000	Net surplus 2013 NZ$000
Cash and cash equivalents +100 bps	7.47	5.43
Cash and cash equivalents – 100 bps	(7.47)	(5.43)

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

APPENDIX A

The complaints process

The complaint process enables us to gather sufficient information to form a view about whether a complaint has substance.

We look for circumstances that indicate there has been a breach of the Privacy Act and which show some harm to the individual who is the subject of the breach.

If we believe that there is substance to a case, we will attempt to facilitate a resolution to the satisfaction of the parties.

Sometimes we will decide not to notify a respondent agency that we have received a complaint about it. This is generally because at an early stage we considered that a complaint had no substance or, after initial contact, the complainant failed to pursue his or her complaint.

Tools to resolve complaints

The Act provides for compulsory conferences between the parties to identify the issues and, where appropriate, to try and resolve them. The Commissioner is able to demand the production of information where it is relevant to an investigation. These statutory tools are being used more routinely.

Systemic issues

We assess complaints for systemic issues that raise wider concerns for the community at large.

Sometimes an individual complaint does not have substance, but reveals systemic practices that may impact on a wider section of the community. In those cases, we may undertake an investigation into that practice or system on our own initiative.

Referral to the Director of Human Rights Proceedings

A complaint that had substance and could not be resolved might also warrant referral to the Director of Human Rights Proceedings who in turn may consider filing a case in the Human Rights Review Tribunal. In the past year, we referred 12 cases to the Director. In some cases, we may have decided that the complaint had some substance but was not sufficiently serious enough to refer to the Director. In those cases, the complainant had the option of taking a case to the Tribunal on his or her own initiative.

An outcome of **'no interference with privacy'** on a complaint usually demonstrates that the agency has met its obligations under the Privacy Act.

A complaint that has **'some substance'** involves a matter where some rectifying response was required by the agency. Some of the cases of substance will have a mixture of issues that involve both a case to be answered and an issue that does not 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.

A complaint that has **'substance'** may range from the need to release further information after our review of the agency's decision, through to an apology and compensation for damages for the effects of a breach of the Privacy Act.

By reporting **referrals to the Director of Human Rights Proceedings**, we aim to influence agencies to avoid proceedings in the Human Rights Review Tribunal. We consistently refer complaints to the Director where an individual's privacy has been interfered with and the matter has not settled. This consistent approach and message is aimed at encouraging parties, especially respondent agencies, to settle a complaint and avoid costly court proceedings.

APPENDIX B

Information matching programme reports

	Compliance
Accident Compensation Act 2001, s.246	
1. IR/ACC Levies and Compensation To identify ACC levy payers, and to calculate and collect premiums and residual claims levies. 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.	√
Accident Compensation Act 2001, s.280(2)	
2. Corrections/ACC Prisoners To ensure that prisoners do not continue to receive earnings-related accident compensation payments. 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.	√
Accident Compensation Act 2001, s.281	
3. ACC/MSD Benefit Eligibility 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. 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. Minor technical issues: In 2013, we reported that programmes at MSD's Integrity Intervention Centre were not operating compliantly because information received from other agencies is not fully destroyed in accordance with section 101 of the Act. While data is removed from view so that it cannot be acted upon, the data resides in MSD's database for up to 2.5 years before a purging process is complete. We met with MSD throughout the year about this issue. Initial work is underway to evaluate the changes required to ensure all programmes operated at the Centre fully comply with destruction requirements.	x
Births, Deaths and Marriages Act 1995, s.78A	
4. BDM(Births)/IR Newborns Tax Number To enable birth information to be confirmed in order to allocate an IRD number to a new-born child. BDM disclosure to IR: The information includes the child's full name, sex, citizenship status and birth registration number. Additionally, the full name, address and date of birth of both mother and father are provided.	√

	Compliance
5. BDM(Births)/MoE Student Birth Confirmation 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. BDM disclose to MoE: Births, Deaths and Marriages provides records of New Zealand-born citizens who were born during the period requested. The records include full name, date of birth, and gender.	√
6. BDM (Births)/MoH NHI and Mortality Register To verify and update information on the National Health Index (NHI) and to compile mortality statistics. 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.	√
7. BDM/MSD Identity Verification 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. BDM disclosure to MSD: BDM provides birth and death information for the 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. Minor technical issues: Refer to programme 3, ACC/MSD Benefit Eligibility.	x
8. BDM (Deaths)/GSF Eligibility To identify members or beneficiaries of the Government Superannuation Fund (GSF) who have died. 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).	√
9. BDM(Deaths)/INZ Deceased Temporary Visa Holders 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. 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.	√
10. BDM (Deaths)/MoH NHI and Mortality Register To verify and update information on the National Health Index and to compile mortality statistics. 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.	√

	Compliance
11. BDM (Deaths)/MSD Deceased Persons To identify current clients who have died so that MSD can stop making payments in a timely manner. 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. Minor technical issues: Refer to programme 3, ACC/MSD Benefit Eligibility.	x
12. BDM (Deaths)/NPF Eligibility To identify members or beneficiaries of the National Provident Fund (NPF) who have died. BDM disclosure to NPF: BDM provides information from the Deaths Register covering the 12 weeks prior to the extraction date. The information includes full name at birth, full name at death, gender, birth date, death date, place of birth, and number of years lived in New Zealand (if not born in New Zealand).	√
13. BDM (Deaths)/NZTA Deceased Drivers Licence Holders To improve the quality and integrity of data held on the Driver Licence Register by identifying licence holders who have died. 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.	√
14. BDM(Marriages)/MSD Married Persons To identify current clients who have married so that MSD can update client records and reassess their eligibility for benefits and allowances. 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. Minor technical issues: Refer to programme 3, ACC/MSD Benefit Eligibility.	x
15. BDM/DIA(C) Citizenship Application Processing To verify a parent's citizenship status if required for determining an applicant's eligibility for New Zealand citizenship. 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.	√
16. BDM/DIA(P) Passport Eligibility 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. 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.	√
17. BDM/IR Child Support Processing To allocate IRD numbers to individuals within the child support scheme, in particular qualifying and dependent children by confirming their birth details. 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.	√

	Compliance
18. BDM/MSD Overseas Born Name Change 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. 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. Minor technical issues: Refer to programme 3, ACC/MSD Benefit Eligibility.	x
Citizenship Act 1977, s.26A	
19. Citizenship/BDM Citizenship by Birth Processing 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. BDM disclosure to Citizenship: For birth registration applications, when no parental birth record can be found, a request is transferred electronically to the citizenship unit to be manually checked against the relevant citizenship records. The information supplied includes the child's date of birth, parent's full names and birth details. Citizenship disclosure to BDM: Citizenship responds to these requests by stating either the type of qualifying record found or that qualifying records were not found.	√
20. Citizenship/DIA(P) Passport Eligibility To verify a person's eligibility to hold a New Zealand passport from citizenship register information. 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.	√
21. Citizenship/INZ Entitlement to Reside To remove from the Immigration New Zealand (INZ) overstayer records the names of people who have been granted New Zealand citizenship. 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.	√
Corrections Act 2004, s.180	
22. Corrections/MSD Prisoners To detect people who are receiving income support payments while imprisoned, and to assist MSD in the recovery of outstanding debts. 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 date, parole eligibility date and statutory release date. Minor technical issues: Refer to programme 3, ACC/MSD Benefit Eligibility.	x

	Compliance
Corrections Act 2004, s.181	
23. Corrections/INZ Prisoners 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. 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.	√
Customs and Excise Act 1996, s.280	
24. Customs/IR Child Support Alerts 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. 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).	√
25. Customs/IR Student Loan Interest 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. 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.	√
26. Customs/Justice Fines Defaulters Alerts 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. Justice disclosure to Customs: Justice provides Customs with the full name, date of birth, gender and Justice unique identifier number of serious fines defaulters for inclusion on Customs' 'silent alerts' or 'interception alerts' lists. 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.	√
27. Customs/MSD Arrivals and Departures 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. 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. Minor technical issues: Refer to programme 3, ACC/MSD Benefit Eligibility.	x

	Compliance
28. Customs/MSD Periods of Residence To enable MSD to confirm periods of residence in New Zealand or overseas to determine eligibility for any benefit. Customs disclosure to MSD: Customs provides MSD access to its CusMod system for verification of departure and arrival dates.	√
29. Customs/IR Student Loan Alerts 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. 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).	√
Education Act 1989, s.128A	
30. MoE/Teachers Council Registration To ensure teachers are correctly registered (Teachers Council) and paid correctly (Ministry of Education). 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).	√
Education Act 1989, ss.226A and ss.238B	
31. Educational Institutions/MSD (StudyLink) Loans and Allowances To verify student enrolment information to confirm entitlement to allowances and loans. 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.	√

	Compliance
Education Act 1989, s.307D	
32. MoE/MSD (StudyLink) Results of Study To determine eligibility for student loans and/or allowance by verifying students' study results. 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, 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. Minor technical 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 Schedule 4 Rule 2 of the Privacy Act 1993. 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. MSD and MoE have committed to changing the algorithm by April 2016.	x
Electoral Act 1993, s.263A and s.263B	
33. Citizenship/EC Unenrolled Voters 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. DIA Citizenship disclosure to Electoral Commission: Citizenship provides full name, date of birth and residential address of new citizens aged 17 years and over (by grant or by descent).	√
34. INZ/EC Unqualified Voters 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. 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 indentified because five separate files are received, each relating to a different permit type.	√
35. NZTA(Vehicle Registration)/EC Unenrolled Voters 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. NZTA disclosure to Electoral Commission: 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.	√
36. MSD/EC Unenrolled Voters 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. MSD disclosure to Electoral Commission: 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.	√

	Compliance
37. NZTA(Driver Licence)/EC Unenrolled Voters 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. NZTA disclosure to Electoral Commission: 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.	√
38. DIA(Passports)/EC Unenrolled Voters 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.. DIA (Passports) disclosure to Electoral Commission: Passports provides full name, date of birth and residential address of passport holders aged 17 years and over.	√
Electronic Identity Verification Act 2012, s.39	
39. DIA Identity Verification Service (IVS) To verify identity information provided by an applicant in support of their application for issuance, 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. 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 still born 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.	√

	Compliance
Housing Restructuring and Tenancy Matters Act 1992, s.68	
40. HNZ/MSD Benefit Eligibility 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. 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. Minor technical issues: Refer to programme 3, ACC/MSD Benefit Eligibility.	x
Immigration Act 2009, s.295	
41. INZ/Justice Fines Defaulters Tracing To enable the Ministry of Justice to locate people who have outstanding fines in order to enforce payment. Justice disclosure to INZ: Justice sends INZ details of serious fines defaulters who have triggered a 'silent' alert as part of the linked Customs/Justice Fines Defaulters Alerts Programme. Each record includes the full name, date of birth, gender, passport number, Justice unique identifier number and flight information of the fines defaulter. INZ disclosure to Justice: INZ supplies information contained on the arrival and departure card, which includes full name, date of birth, gender, passport number, nationality, occupation, New Zealand address and date of expected return to New Zealand (in the case of a departing traveller). Minor technical issues: In August 2013 Justice was granted a 12 month approval to transfer information online on condition that file encryption be implemented by 31 December 2013. Justice failed to implement the required safeguard so was in breach of the online approval. That approval has now expired. Justice has ceased transferring information online until agreed safeguards are in place and a new approval is granted by this Office.	x
Immigration Act 2009, s.300	
42. INZ/MoH Publicly Funded Health Eligibility 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. 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.	√

	Compliance
Motor Vehicle Sales Act 2003, ss.120 and 121	
43. Customs/MBIE Motor Vehicle Traders Importers To identify people who have imported more than three motor vehicles in a 12 month period and are not registered as motor vehicle traders. 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.	√
Motor Vehicle Sales Act 2003, ss.122 and 123	
44. NZTA/MBIE Motor Vehicle Traders Sellers To identify people who have sold more than six motor vehicles in a 12-month period and are not registered as motor vehicle traders. 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 NZTA: 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.	√
Social Security Act 1964, s.126A	
45. MSD/Justice Fines Defaulters Tracing To enable the Ministry of Justice to locate people who have outstanding fines in order to enforce payment. 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. Substantive issue: In 2013 we reported this programme as non compliant because information was not being destroyed in accordance with the conditions contained in the information matching agreement. Justice is yet to implement the required changes but has provided assurances that it will do so by 30 November 2014.	x
Social Security Act 1964, s.126AC	
46. Justice/MSD Warrants to Arrest To enable MSD to suspend or reduce the benefits of people who have an outstanding warrant to arrest for criminal proceedings. Justice disclosure to MSD: Justice provides MSD with the full name (and alias details), date of birth, address, Justice unique identifier and warrant to arrest details. Minor Technical Issue: Information received from Justice is not fully destroyed in accordance with section 101 of the Act. While data is removed from view so that it cannot be acted upon, the data resides in MSD's database for up to 18 months before a purging process is complete. Initial work is underway to evaluate the changes required to ensure the programme operates compliantly.	x

	Compliance
Social Welfare (Transitional Provisions) Act 1990, ss.19C and 19D and Social Welfare (Reciprocity with Australia) Order 2002, Article 18	
47. Centrelink/MSD Change in Circumstances For MSD and Centrelink (the Australian Government agency administering social welfare payments) to exchange benefit and pension applications, and changes of client information. 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. Minor Technical Issue: Copies of files were not always being deleted in the required timeframe. The manual process has now been replaced with an automated process and this has corrected the issue.	x
Social Welfare (Transitional Provisions) Act 1990, ss.19C and 19D and Social Welfare (Reciprocity with the Netherlands) Order 2003, Article 216	
48. Netherlands/MSD Change in Circumstances To enable the transfer of applications for benefits and pensions, and advice of changes in circumstances, between New Zealand and the Netherlands. 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.	√
49. Netherlands/MSD General Adjustment To enable the processing of general adjustments to benefit rates for individuals receiving pensions from both New Zealand and the Netherlands. 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.	√
50. IR/MSD(Netherlands) Tax Information To enable income information about New Zealand-resident clients of the Netherlands government insurance agencies to be passed to the Netherlands for income testing. 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.	√

	Compliance
Tax Administration Act 1994, s.82	
51. IR/MSD Commencement Cessation Benefits To identify individuals receiving a benefit and working at the same time. MSD disclosure to IR: Each record 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. Minor technical issues: Refer to programme 3, ACC/MSD Benefit Eligibility.	x
52. IR/MSD Commencement Cessation Students To identify individuals receiving a student allowance and working at the same time. MSD disclosure to IR: 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. Minor technical issues: Refer to programme 3, ACC/MSD Benefit Eligibility.	x
Tax Administration Act 1994, s.83	
53. IR/MSD Community Services Card To identify people who qualify for a Community Services Card (CSC) based on their level of income and number of children. 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.	√
Tax Administration Act 1994, s.84	
54. MSD/IR Working for Families Tax Credits Double Payment To identify individuals who have wrongly received Working for Families Tax Credits (WfFTC) from both MSD and IR. 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.	√

	Compliance
Tax Administration Act 1994, s.85	
55. IR/Justice Fines Defaulters Tracing To enable the Ministry of Justice to locate people who have outstanding fines in order to enforce payment. Justice disclosure to IR: Justice selects fines defaulters for whom it has been unable to find a current address, and sends the full name, date of birth, and 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. Substantive issue: In 2013 we reported this programme as non compliant because information was not being destroyed in accordance with the conditions contained in the information matching agreement. Justice is yet to implement the required changes but has provided assurances that it will do so by 30 November 2014.	x
56. MSD/IR Working for Families Tax Credits Administration 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). 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.	√

Online transfer approvals

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

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

The following table shows first time approvals and other approvals reviewed during the reporting year.

FIRST TIME APPROVALS

User agency Programme name Approval date	Reason for granting	Grounds in support
Inland Revenue		
Newborns tax number 11 October 2013	Efficiency and security	Auditing enabled
Ministry of Social Development		
Warrants to arrest 10 July 2013	Efficiency and security	Timely delivery of data

RENEWED APPROVALS

User agency Programme name Approval date	Reason	Grounds
DIA		
Citizenship by birth processing 18 March 2014	Efficiency and security	Satisfactory audit result
DIA – Identity Verification Service		
Identity verification (BDM) 18 April 2014	Efficiency and security	Timely delivery of data
Identity verification (Citizenship) 18 April 2014	Efficiency and security	Satisfactory audit result
Identity verification (Passports) 18 April 2014	Efficiency and security	Timely delivery of data
Identity verification (Immigration) 18 April 2014	Efficiency and security	Satisfactory audit result
Electoral Commission		
Unqualified voters 9 October 2013	Efficiency and security	Auditing enabled
Ministry of Justice		
Fines defaulters (Customs) 27 August 2013	Efficiency and security	Auditing enabled
Fines defaulters (Immigration) 27 August 2013	Efficiency and security	Satisfactory audit result
Ministry of Social Development		
Arrivals and departures 9 July 2013	Efficiency and security	Satisfactory audit result
Benefit eligibility (Housing) 25 September 2013	Efficiency and security	Auditing enabled
Change in circumstances (Centrelink) 16 December 2013	Efficiency and security	Satisfactory audit result
Periods of residence (Customs) 16 December 2013	Efficiency and security	Satisfactory audit result
Verification of study 16 June 2014	Efficiency and security	Timely delivery of data
Results of study 16 June 2014	Efficiency and security	Satisfactory audit result