PRIVACY COMMISSIONER ANNUAL REPORT

2015

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 2015

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

November 2015

THE MINISTER OF JUSTICE

I tender my report as Privacy Commissioner for the year ended 30 June 2015

John Edwards
Privacy Commissioner

CONTENTS

FIGURES AND TABLES

APPENDICES

Key points

Outreach and communications

- We launched online education modules. We created these modules in collaboration with online training specialists LearningWorks.
- Our enquiries team handled 8,372 enquiries from the public through our 0800 phone line and email.
- We received 273 media enquiries covering a wide range of topics including data breaches, the Harmful Digital Communications Act, unmanned aerial vehicles (UAVs) or 'drones', and property ownership information on public registers.
- We worked with the Department of Internal Affairs and Victoria University to hold the Identity Conference at Te Papa in Wellington in May. The two day conference featured a high quality line-up of local and international speakers and was attended by 300 people.
- Our blog attracted about 1,000 visits a week from readers. It continues to be an effective way to highlight privacy topics raised by Human Rights Review Tribunal decisions, news media stories and case notes.
- Staff from the Office presented at a range of conferences, seminars and industry groups throughout the year. Many of these presentations were in regional New Zealand, addressing influential business, health and media audiences in Dunedin, Palmerston North, Hamilton and the Hawkes Bay.
- Our programme of Technology and Privacy Forums continued throughout the year. We held six forums, all of which were well attended.

Dispute resolution and investigations

- We made significant efforts to modernise our complaints processes in order to resolve cases faster. We have increased our use of alternative dispute resolution techniques, including an increased readiness to bring complainants and respondents together in person or by phone.
- We closed 827 complaint files which was an increase from 702 last year. Of these, 44 percent were closed with a settlement between the parties – up from 32 percent the previous year.
- We have implemented a complaints lodgement system through our website, which uses encryption software so that people can make a complaint to us online in a secure way.
- In order to increase the consequences for not complying with privacy obligations, we adopted a naming policy. This is a policy of publicly naming some agencies when they do not comply with the Privacy Act. The policy was implemented this year after a consultation period in December 2014.
- The Harmful Digital Communications Act came into force and changed certain aspects of the Privacy Act. Complaints that were previously outside the ambit of the Privacy Act because of the section 56 'domestic affairs exemption' can now be investigated. This has expanded the nature of complaints people can make to us, particularly those who suffer harm through the online actions or use of digital communications by others.

Research & analysis

- The Office launched its inaugural $75,000 Privacy Good Research Fund. We received 14 applications. Each successful applicant could be awarded up to $25,000 for an individual privacy-related research project.
- We appointed a senior staff member responsible for finance & performance to build our capacity in internal and external reporting.

Policy and technology

- We undertook policy work with a number of stakeholders to prepare for the upcoming Privacy Act reform. These changes will bring the Act up to date with the current technological and international environment, as well as give the Privacy Commissioner stronger enforcement tools.
- Effective information sharing forms a key component of the Government's Better Public Services objective. We helped to facilitate this objective through Approved Information Sharing Agreements (AISAs). We assisted in the formation of an AISA between agencies for the Vulnerable Children's Hub.
- Our office provided advice and feedback for a range of public sector organisations. We supported Customs on proposed changes to the Customs and Excise Act, reviewed Police vetting services in conjunction with Police and the Independent Police Conduct Authority, and made a submission supporting the minimal privacy impact of the Health and Safety Reform Bill.
- We launched our *Sharing Personal Information about Families and Vulnerable Children* guide and an interactive escalation ladder tool to assist multi-agency teams that work with vulnerable children.
- In an ongoing effort to make privacy easy, we published privacy guidance material including a Privacy Impact Assessment toolkit, a guide on Approved Information Sharing Agreements (AISAs) and launched our online *Priv-o-Matic* privacy statement generator.
- We advised the Data Futures Forum on using data while maintaining privacy. The Data Futures Forum is now the Data Futures Partnership. We support the direction of the Partnership and will continue our engagement to ensure that the Government and private sector can continue to innovate and safely realise the value of administrative data sets.
- We played a similar role in the Statistics New Zealand's addition of data from the Ministries of Health and Justice to the Integrated Data Infrastructure.
- We made an amendment to the Credit Reporting Credit Code, restricting credit reporters to a charge of no more than $10 for consumers seeking their credit information.

Data breaches

- Breach notifications remain voluntary but we expect breach reporting to become mandatory when the Privacy Act is reformed. As in previous years, the most common feature among the reported breaches was human error or carelessness.
- We continued to receive a significant number of voluntary data breach notifications. During the year, we received 121 notifications, with 71 from the public sector and 50 from the private sector.

International

- The Privacy Commissioner was appointed Chair of the Conference Committee for organising the International Conference of Data Protection and Privacy Commissioners (ICDPPC) in Amsterdam in October 2015.
- Our office assumed Secretariat duties for the ICDPPC, including establishing a website for the Amsterdam conference.
- We contributed to a review of the APEC privacy framework.
- We continued in our role as Administrator of the Cross Border Privacy Enforcement Arrangement.
- We participated in the annual Global Privacy Enforcement Network (GPEN) sweep, which this year targeted the privacy practices of websites and mobile apps used by or popular with children.

Introduction

In 2014/15 we introduced new initiatives and pursued new approaches. We encouraged the practice of working across teams. We expanded our range of services by developing online resources, such as training modules, an online complaint form and a privacy statement generator. Our dispute resolution teams made concerted efforts to ensure that matters were resolved swiftly and effectively. Our policy expertise was called upon to assist agencies, particularly in the social sector, who wanted to share personal information to provide better services to individuals.

Continued interest and awareness of the activities of intelligence and surveillance agencies led us to initiate a regular oversight group. The membership of that group is made up of the Inspector General of Intelligence and Security, the Chief Ombudsman, the Auditor General and the Privacy Commissioner. The group meets quarterly.

We are also working with the Inspector General of Intelligence and Security to develop opportunities for dialogue at an international level amongst privacy regulators and other oversight agencies.

Making privacy easy

A key focus this year was to 'make privacy easy' – for private sector organisations, public sector agencies and individuals. This is an ongoing effort to equip people with practical tools and resources to stay on top of their own privacy rights and obligations. For example, we built an online privacy statement generator, published a privacy impact assessment toolkit and created a directory of privacy professionals. We published these tools online in order to make them widely accessible and to encourage business and individual uptake of online government services.

Privacy matters

The Human Rights Review Tribunal issued judgments that highlighted the growing value of privacy in our society. *Hammond v NZCU Baywide* awarded the complainant a record-breaking $168,000 in damages. *Taylor v Orcon* awarded the complainant $25,000 for the difficulties the complainant had suffered as a result of incorrect information on his credit record. These two cases indicate that the financial cost to respondents of a privacy breach may be increasing.

Faster and more effective complaints resolution

We made significant changes to our complaints investigation process in order to resolve cases faster and more effectively. The key change was a move to resolve complaints through phone and email when possible. While written correspondence and legal opinions are necessary for some cases, they are not necessary for all complaints. Resolving cases through less-formal means, where appropriate, helps us deliver better outcomes overall by freeing up capacity.

We also enabled people to make privacy complaints easily and securely through an online complaints lodgement tool.

Getting the parties talking

During the year, we made greater use of our statutory ability to bring complainants and respondents together through compulsory conferences. These meetings can have the benefit of helping to define the scope of an investigation by clarifying its focus on specific issues. We also use it as an opportunity to try and find a mediated resolution where possible. We have found that the face-to-face facilitated discussion helps both complainants and respondents quickly reach agreement on issues.

Naming policy

We have increased accountability for agencies that get things wrong. An example of this is our naming policy. The naming policy includes a clear set of criteria indicating when we publicly name organisations not complying with their privacy obligations. We adopted this policy after a consultation period in December 2014, and formally adopted it in early 2015. Going forward, we will continue to seek feedback and amend the policy as and when appropriate.

Taking education online

We launched an online education facility to make it easier for people to get up-to-speed with their privacy obligations without having to attend a half-day course. We added an online delivery model in order to scale up the impact of our existing in-person education and training and to enable the training to be accessed from anywhere. We have trained more people, faster by giving them access to privacy education online, at their own pace. We continue to add new courses to meet specific needs and deepen peoples' privacy understanding.

Better public services

Our office contributed towards achieving Better Public Services goals. Our contributions were focused on making activities easier by both enhancing organisations' ability to share information and strengthening trust in public sector organisations' ability to do so. Some of these are outlined below.

Easier information sharing

Effective information sharing is central to the Better Public Services goal of supporting vulnerable children. We directly contributed to this objective by helping to develop an Approved Information Sharing Agreement (AISA) between many agencies to support the Child Protection Teams. This agreement empowered social service agencies to quickly share information between one another to identify at-risk children.

We also built an online tool for front-line staff to help them determine whether they can share information, how much they can share and with whom. This tool – called the *Escalation Ladder* – is available on our website.

We also published guidance to help more agencies share information with one another. Examples include a *Guide to Approved Information Sharing Agreements and a Privacy Impact Assessment Toolkit*.

Building trust in online engagements

In order to encourage people to engage with organisations online, people need to be able to trust those organisations with the information they hold. We helped to build this trust by working with government agencies on privacy impact assessments, consulting on policy and submitting on legislation. By highlighting and explaining privacy risks, we helped to give individuals and businesses the assurance they need to engage with organisations online.

Everyone is a publisher

Connected devices are nearly ubiquitous, giving people an unprecedented ability to create and publicise information. The Harmful Digital Communications Act (HDCA), which passed into law in June, aims to

reduce the harm people can cause one another through digital communications. The HDCA brought welcome changes to the Privacy Act by limiting both the 'publicly available' and 'domestic affairs' exceptions to the Act in certain circumstances. Cases involving 'revenge porn' are one such example.

Outreach

Outreach this year included a focus on encouraging online interactions. We continued to actively engage on social media, post blog posts and promote guidance material online in an effort to help people get the information they need through online channels.

We also gave a significant number of speeches and presentations. A number of these were in towns and cities outside the main centres of Wellington, Auckland and Christchurch. This was part of an ongoing effort to raise privacy awareness across the country. We expect our shift to online guidance, tools and education to support our regional outreach efforts.

Big data, big oversight

We provided significant guidance and oversight at a macro level. The Data Futures Forum was a government initiative to find ways to use data to benefit society. We advised the Forum on how to get the most out of this data while also maintaining respect for individual privacy. The Data Futures Forum is now the Data Futures Partnership. We support the direction of the Partnership and look forward to engaging with it on an ongoing basis.

We played a similar role in the Statistics New Zealand's addition of data from the Ministries of Health and Justice to the Integrated Data Infrastructure.

International relationships

International relationships remain important as people have gained the ability to easily move large amounts of data across borders. Significant activities included New Zealand becoming Chair of the Conference Committee for the International Conference of Data Protection and Privacy Commissioners and maintaining our role as Administrator of the Cross Border Privacy Enforcement Arrangement (CPEA). The CPEA is an enforcement arrangement while the international conference focusses on capacity building and strategic work. Our strong connections with other regulators across the Asia Pacific are maintained through the regular Asia Pacific Privacy Authorities (APPA) network and meetings.

Law reform

We undertook significant policy work with a number of stakeholders to prepare for the upcoming Privacy Act reform. These changes will bring the Act up to date with the current technological and international environment. Key anticipated 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 requestors 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.

Looking forward

We are cautiously optimistic about the way agencies are collecting, using and sharing information. We've seen more agencies adopting a 'privacy by design' perspective, undertaking privacy impact assessments and engaging with our office at a very early stage of projects that involve personal information. However, there is more work to be done! We are looking forward to engaging with more agencies on privacy projects, as well as making use of the new tools and resources we expect from the upcoming law reform.

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 so much an ordinary daily feature of business and personal life. In addition to changes in business processes such as outsourcing, cloud computing and off-shoring, individuals now publish, not just consume, content online. The internet and mobile computing technology has made it easier than ever for individuals to post information about themselves and others to the world. Global privacy enforcement authorities need to cooperate across borders to protect against privacy threats wherever they originate from. Collaboration with counterpart authorities can lead to enhanced problem solving, creative policy solutions and more effective regulation.

The Office engages with overseas counterparts in a number of ways. For example:

- International collaboration can lead to common standards to facilitate business transactions across borders in ways that protect the interests of individuals.
- A company's actions in one country can affect the citizens in another. In the event of a security breach, we may need to seek the cooperation of overseas enforcement authorities.
- Other countries may encounter privacy challenges before they affect New Zealand and we hope to gain 'advance warning' through their experience.

The Office engages in a variety of forums, principally:

- Asia Pacific Privacy Authorities (APPA) Forum
- International Conference of Data Protection and Privacy Commissioners (ICDPPC)
- APEC: Data Privacy Subgroup (DPS)
- OECD: the Working Party on Security and Privacy in the Digital Economy (SPDE).

Some of the highlights of 2014/15 were:

- **International Conference of Data Protection and Privacy Commissioners:** at the 36th International Conference, the New Zealand Privacy Commissioner was elected as Chair of the Conference's Executive Committee and in this capacity the Office of the Privacy Commissioner provided the Conference Secretariat. This has provided an opportunity to substantially contribute to advancing capacity building and strategic work amongst data protection authorities at an international level. A significant milestone was building a permanent Conference website.
- **Asia Pacific Privacy Authorities Forum (APPA):** we participated in the 42nd and 43rd Forums in Vancouver and Hong Kong. The APPA Forum is continuing to build its importance in the region.
- **Global Privacy Enforcement Network (GPEN):** The network remains a key means of connecting with our international counterparts in enforcement. The network has grown to 53 authorities in 39 economies. We stood down from the GPEN Committee in 2015 due to the need to concentrate available resources on performing our role as Secretariat of the International Conference of Data Protection and Privacy Commissioners.
- **APEC Cross-border Privacy Enforcement Arrangement (CPEA):** The arrangement now connects 25 privacy enforcement authorities in 10 APEC economies. We continued as a CPEA Administrator.
- **APEC DPS:** New Zealand took the lead in undertaking a review of the APEC Privacy Arrangement. In January 2015 our office presented a paper recommending updates to the APEC Privacy Framework drawing upon recent work undertaken in the OECD.

Media, outreach & education

New approach for education and training

We reviewed the way we were delivering education and training. Our practice had been to deliver face-to-face training to small groups in scheduled workshops throughout the year. These training sessions were held in Auckland and Wellington, with less regular sessions in Christchurch. We were conscious that this approach meant it was difficult for people outside the main centres to access privacy training. We commissioned online training specialists, LearningWorks, to develop a series of training modules. The first two modules were launched during Privacy Week 2015 and have been well received. We are continuing to develop further modules covering different topic areas. We are working with the Government Chief Privacy Officer in developing some of the modules aimed at public sector audiences. The online training is free and can be accessed through our website: **www.privacy.org.nz/e-learning**

Regional visits

In the past year, we have been able to schedule visits to other parts of New Zealand to meet with stakeholders in those centres. These are very useful engagements that enable our staff to hear concerns directly from stakeholders and allow us to reach audiences that we would not otherwise. We often coordinate with a partner organisation, such as a chamber of commerce, or a community law centre, to assist in setting up public presentations or clinics in the centres.

Media

Media interest and enquiries continued to be strong throughout the year (273 enquiries in 2014/15). These enquiries cover a wide range of topics including, for instance, Unmanned-Aerial Vehicles (UAVs) or 'drones', anti-terrorist legislation; and the sharing of images on social media. We are sometimes directing journalists to the range of experts listed in our Directory of Privacy Professionals for comment.

We maintained an active blog throughout the year, with very regular posts on topical issues. We have found the blog to be an effective vehicle to raise awareness of privacy debates in the media and to publicise case notes.

Outreach

Staff from the Office continued to present at a range of conferences, seminars and industry groups throughout the year. There are numerous requests and while we are not able to fulfil them all, we try and meet priority areas. For instance, in the last year, we have been active in supporting the work of the Children's Action Teams throughout New Zealand. We hope that in time, some of this demand may be met by privacy professionals such as those listed in the Directory of Privacy Professionals. Our series of Technology and Privacy Forums continued throughout the year and are consistently well attended.

Publications

We released several new guidance publications during the year. The guidance on *Sharing Personal Information about Families and Vulnerable Children* includes an escalation ladder tool to assist those working with families to decide when and how to share personal information. The escalation ladder can be used online as an interactive tool.

We also released a Privacy Impact Assessment (PIA) Handbook and, earlier in the year, guidance on Approved Information Sharing Agreements. All publications are available on our website: **www.privacy.org.nz**

Enquiries

The Office handled 8,372 enquiries from the public through our 0800 phone line and email during the year. The enquiries service is a valuable gauge of public concern and interest in privacy. We are continuing to look at ways to analyse the subject and nature of the enquiries we receive. We are looking at improving the ways that enquirers can easily find the information they need through our website.

Privacy Week

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

A highlight of the week was an exhibition of privacy-themed art works created by the artists at Vincents Art Workshop in Wellington. The art works were later auctioned through Trade Me, with the funds directed to Vincents.

During Privacy Week we launched the first two modules in our online privacy training: Privacy 101 and Health 101. Both are free to use and are available at: **www.privacy.org.nz/e-learning**

Our Office coordinated with our APPA colleagues to develop the 'Privacy Matters' poster series that was used by APPA members across the region. A series of seminars and activities ran during the week.

The Identity conference 2015 – *Enabling Digital Identity and Privacy in a Connected World* – took place at Te Papa shortly after Privacy Week. This successful event, jointly organised with Victoria University, Department of Internal Affairs and Office of the Privacy Commissioner, brought together a range of international and New Zealand speakers on topics such as data analytics, privacy by design, the internet of things and cybercrime.

Investigations

This year we undertook significant efforts to change our complaints processes in order to resolve cases faster and deliver higher satisfaction levels. This is an ongoing process, and we are moving in the right direction: 44% of our cases were closed with a settlement between the parties (up from 32% last year) and we closed 827 complaint files – an increase from 702 last year.

Blitz to free up capacity

We came into the year with some complaints that were more than two years old. Long investigations created a poor experience for those involved. To clear this backlog, we had a complaints 'blitz' in early 2015. Investigators worked hard in a focus on older cases. The effect was that we halved the number of cases that were more than 6 months old and created the capacity we needed to move to a new way of working.

At the end of the financial year, we had closed or settled 85% of our complaints that were 9 months old or older. This was on target but slightly lower than the 88% we closed or settled the year before. We expect to raise this number in the future as our new approaches bed in.

Changing our communications channels

In the past, most of our complaints investigations were carried out by letter. This year, we prioritised phone and email contact. We adopted this strategy because we recognised that a significant number of cases do not require formal legal opinions – and can consequently be resolved significantly faster.

We also implemented an online complaints tool on our website, making it easier for people to submit privacy complaints. Twenty-eight percent of our complaints came through this channel this year.

While we have focussed on different channels, the more complex cases do still require written correspondence. This year we focussed on identifying the complex cases from those less-complex cases and reaching early resolution when possible. The goal of this case management approach was to deliver faster resolution for all our cases by quickly resolving the less-complex cases and in turn freeing up resources to deliver a quicker resolution for the more-complex cases.

Areas to improve

The shift in how we approach complaints is an ongoing process that will continue into the next financial year. Our intention is not just to focus on speed but also high levels of satisfaction – both from complainants and respondents. This is an area where we will focus our efforts in the coming year, as our overall satisfaction level was 53%, where our target was 80% satisfaction. An independent audit of a sample of our complaint files rated 57% at 3.5 out of 5 or higher – a figure which fell short of our target of 70%. The quality of the investigations was seen as high, but investigations lost points for timeliness and lack of procedural

clarity. We expect to see improvement in this area as we continue to adopt fast-resolution strategies and commission a procedures manual to clarify and standardise our investigation processes.

Complaints received by agency type

SECTOR	NUMBER	PERCENTAGE
PUBLIC	514	61.56%
PRIVATE	321	38.44%

Settlement outcome

SETTLEMENT OUTCOME	NUMBER
INFORMATION RELEASED	141
APOLOGY	56
INFORMATION PARTLY RELEASED	93
MONEY/MONIES WORTH	27
INFORMATION CORRECTED	24
ASSURANCES	32
CHANGE OF POLICY	15
TRAINING	5

Litigation

Most complaints are resolved during the course of the investigation through some form of settlement. When cases cannot be settled, we have the option of referring the matter to the Director of Human Rights Proceedings, who may choose to take the case to the Human Rights Review Tribunal. Complainants also have the right to take their case to the Tribunal themselves.

This year we referred two cases to the Director – the lowest number in a number of years, and down from 12 in the 2013/2014 financial year. The Director took proceedings in one of the cases and is still considering the other one. These are in addition to cases currently under consideration or litigation from previous years.

Twenty-four complainants took proceedings to the Tribunal without a referral from us. The Tribunal found an interference with privacy in eight (8) different cases this year, and found no interference in two cases.

Notable Tribunal decisions

The Tribunal issued two particularly notable decisions that set strong precedents for future decision-making.

The first of these decisions was *Hammond v NZCU Baywide*. In this case, a woman celebrated her resignation from a job by having a small party and baking a cake with a rude statement on it. A photo of the cake was posted to Facebook. When her past employers heard about the photo, they pressured one of the woman's Facebook friends to take a screenshot and send it to them; they then distributed the screen shot to a variety of recruiters, as well as her new employer. The woman lost her new job and was unable to find another one because of the 'smear' campaign.

We found an interference with privacy and referred her case to the Director of Human Rights Proceedings, who chose not to take the case. She took the case to the Tribunal herself, and was ultimately awarded record-setting damages of $168,000.

The second was *Taylor v Orcon*. In this case, Mr Taylor complained that telecommunications company Orcon had passed incorrect information about his unpaid debt to debt collection agencies. This affected Mr Taylor's credit rating and made it difficult for him to find rental accommodation, causing him significant stress, humiliation and hurt feelings. The Tribunal found that the incorrect debt did not need to be the sole cause of Mr Taylor's harm to create an interference with privacy (and with it liability). Rather, the fact that it was one cause was sufficient. The Tribunal awarded Mr Taylor $25,000 in damages.

Codes of practice

At the start of the year there were six Codes of Practice in force. We amended two codes: the Justice Sector Unique Identifier Code and the Credit Reporting Privacy Code. In both cases, the work developing, notifying and taking submissions on the codes was carried out in the 2013/2014 year and were fully reported in last year's Annual Report. The amendments were finally issued at the beginning of 2014/15 year in July 2015.

The amendment to the Justice Sector Unique Identifier Code made no substantive changes to the code but simply assured that the code's definition remained in line with other legislation.

The Credit Reporting Privacy Code generally provides that a credit reporter may make no charge for giving access to individuals to information about themselves. However, in limited circumstance the code allows for a reasonable charge to be made. The amendment to the code imposed a maximum charge limit.

Policy

The Office's policy function supports improved privacy practices in a number of different ways:

- advising Cabinet and Parliament on the privacy implications of legislative proposals and other policy initiatives
- advising government agencies and private organisations on the privacy implications of policy initiatives
- producing tools and guidance to help people and organisations 'self-serve' policy advice.

Service-oriented advice

This year marked a major shift in our policy approach, as we worked to provide consultation and feedback at a very early stage in policy initiatives. The objective was to provide practical privacy advice at a stage in the project where it could be implemented relatively easily. We credit this approach for our high satisfaction rating – 96% of recipients of our policy advice were satisfied, a significant margin above the 70% target.

We are increasingly taking the opportunity to explain how we have influenced policy by appearing in front of Cabinet and Select Committees in support of improved policies, rather than only appearing when we disagree. This approach has been well-received.

Engaging the private sector

Private sector organisations are holding an increasingly large amount of information about the people they work with. To this end, we committed a significant amount of resource towards improving our engagement with private sector organisations. The first half of the year was essentially a 'needs analysis,' engaging with organisations to determine what kind of guidance they needed and how we could best deliver it. In the second half of the year, we delivered guidance and tools based on this analysis, such as the Priv-o-Matic, an automated privacy statement generator.

We also published a strategy for engaging with the private sector about how they use technology. Private sector agencies play a crucial role in innovation, and are at the forefront of both technology adoption and exploring new ways to use data. Our strategy positions us to create ongoing relationships with private sector organisations, so we are involved in privacy conversations at a very early stage.

Helping vulnerable children

Supporting vulnerable children is a key 'Better Public Services' goal. We contributed to this goal in a significant way by advising on the Approved Information Sharing Agreement for Improving Public Services for Vulnerable Children. This legal agreement allows agencies involved in the Vulnerable Children's Hub (the point of contact for practitioners and professionals who have concerns about a vulnerable child) to share information to identify vulnerable children and refer them to the most appropriate support. The agreement helps agencies to deliver services faster while also maintaining individual privacy and trust.

We also made an escalation ladder for social services professionals. This tool helps people quickly determine when it's appropriate to use, collect or disclose information about vulnerable children.

Big data

Public sector agencies have an opportunity to deliver significantly better services by harnessing the data that individuals and organisations are generating. We helped to facilitate this opportunity by advising on the privacy implications of key 'big data' projects.

The Data Futures Partnership is a cross-disciplinary project to find ways to get more value out of data and deliver better public services. Our submission supported its 'principles' approach and highlighted the role the Privacy Act plays in protecting the rights of individuals in 'big data' scenarios.

In a similar vein, the Integrated Data Infrastructure is a Statistics NZ-led project to combine data from a variety of government agencies. We were consulted on a project to add justice and health information to this infrastructure, advising the organisation on data encryption practices to reduce the risk of inadvertent privacy breaches during the data transfer process.

Public sector policy advice

As always, we provided a significant amount of advice and feedback for public sector organisations. Key projects this year included:

- Supporting Customs to draft discussion documents on proposed changes to the Customs and Excise Act.
- A submission on the Productivity Commission's 'More Effective Social Services' report. We agreed that agencies can deliver better social services by sharing information, but argued that any information sharing should only be carried out to the degree necessary to accomplish appropriate social goals.
- A submission on the Law Commission's review of the Extradition Act and Mutual Assistance in Criminal Matters Act, advocating for transparency and privacy safeguards in the Act.

Breach notifications

We continued to receive a significant number of data breach notifications through the year. Breach reporting remains voluntary, so there is no way of knowing what proportion of actual breaches are reported to our office.

Mandatory breach reporting is expected to be part of the Government's reform of the Privacy Act. It will help us prevent more data breaches by giving a better view of data breaches overall. This will in turn enrich the advice we provide to mitigate breaches.

As in previous years, the most common feature among the reported breaches was human error or carelessness. Nearly half of the reported data breaches involved information being sent to the wrong entity or sent out in the wrong form. These types of error were fairly evenly divided between physical and electronic forms (e.g. email).

NUMBERS OF NOTIFICATIONS AND SECTOR WHICH NOTIFICATIONS CAME FROM

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	116	90	26
14/15	121	71	50

2013/14 figures are slightly different from those previously reported. Considerable effort has been applied to correcting the metadata, and that may explain the change in numbers.

MOST COMMON TYPES OF BREACHES NOTIFIED

TYPES OF BREACH	2012/13	2013/14	2014/15
WEBSITE PROBLEM	12	6	10
LOSS/THEFT OF PHYSICAL FILE	5	15	20
LOSS/THEFT OF PORTABLE STORAGE DEVICE	7	1	5
EMPLOYEE BROWSING	6	1	6
ELECTRONIC INFORMATION SENT TO WRONG RECIPIENT	17	27	36
PHYSICAL INFORMATION SENT TO WRONG RECIPIENT	23	23	24

Information matching

Review of the way agencies notify individuals

This year we initiated a project with the objective of raising transparency and public awareness about information matching programmes. The project focused on checking and improving agency practice in two areas:

- informing the public about the operation of each programme
- notifying individuals subject to adverse action (such as a reduced benefit) by sending written notices.

Our review found that all programmes had some form of general notification but there were some opportunities to improve practices. ACC made changes to improve its notification for one programme and MSD has committed to work with us towards general notification for several programmes.

We were satisfied with the majority of the adverse action notices. Only two programmes did not meet the requirements. MSD has implemented changes for one of these programmes. The other, the MSD/IR Working for Families Tax Credits Administration programme, has an ongoing technical compliance issue which is described in the programme report in Appendix B.

Data destruction issues remedied

Organisations are remedying problems with data destruction. In 2013 we reported that ten programmes at MSD's Integrity Intervention Centre were not compliant with destruction rules because information was removed from view but not fully destroyed. In June, MSD confirmed that system changes have been made to comply with destruction rules.

Two programmes operated by the Ministry of Justice were also identified as not compliant with destruction rules in the 2013 review. In February 2015, the Ministry informed us that it had modified its data retention processes in order to comply with the Act.

Changes in authorised and operating programmes

Parliament passed no new information matching authorisations during the year. The HNZ/MSD Benefit Eligibility programme ceased operation in August 2014. The Malta/MSD Social Welfare Reciprocity programme was authorised in September 2013 and reporting on activity commenced in 2014/15.

Office and functions

Independence and competing interests

The Privacy Commissioner has wide ranging functions. The Commissioner 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 the Commissioner 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 (Policy & Operations) has responsibility for investigation teams in both offices; and for enquiries, policy and technology advice and information matching work.

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

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

The General Counsel is legal counsel to the Privacy Commissioner, manages litigation and gives advice in the area of investigations.

EEO profile

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.

WORKPLACE GENDER PROFILE

	WOMEN		MEN		TOTAL
	FULL-TIME	PART-TIME	FULL-TIME	PART-TIME	
COMMISSIONER			1		1
SENIOR MANAGERS	2		2		4
TEAM LEADERS/SENIOR ADVISERS	4	1			5
INVESTIGATING OFFICERS	5		3		8
ADMINISTRATIVE SUPPORT	5	2			7
ADVISERS (TECHNOLOGY, POLICY AND COMMUNICATIONS)	5		6		11
ENQUIRIES OFFICERS	1	1			2
TOTAL	22	4	12		38

WORKPLACE ETHNIC PROFILE

	MAORI		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									4	
TEAM LEADERS/SENIOR ADVISERS					1				3	1
INVESTIGATING OFFICERS	1		1						5	
ADMINISTRATIVE SUPPORT									5	2
ADVISERS (TECHNOLOGY, POLICY AND COMMUNICATIONS)					1		1		10	
ENQUIRIES OFFICERS									1	1

We do not collect information on employees' age or disabilities. If a disability is brought 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.

Finance and Performance Report

FOR THE YEAR ENDED 30 JUNE 2015

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 performance, and for the judgements made in them.

We are responsible for any end-of-year performance information provided by the Privacy Commissioner under section 19A of the Public Finance Act 1989.

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 performance reporting.

In the opinion of the Privacy Commissioner, these financial statements and statement of performance fairly reflect the financial position and operations of the Privacy Commissioner for the year ended 30 June 2015.

Privacy Commissioner
J Edwards
21 October 2015

General Manager
G F Bulog
21 October 2015

AUDIT NEW ZEALAND
Mana Arotake Aotearoa

Independent Auditor's Report

To the readers of the Privacy Commissioner's financial statements and performance information for the year ended 30 June 2015

The Auditor-General is the auditor of the Privacy Commissioner. The Auditor-General has appointed me, Athol Graham, using the staff and resources of Audit New Zealand, to carry out the audit of the financial statements and the performance information, including the performance information for an appropriation, of the Privacy Commissioner on her behalf.

Opinion on the financial statements and the performance information

We have audited:

- the financial statements of the Privacy Commissioner on pages 35 to 50, that comprise the statement of financial position as at 30 June 2015, the statement of comprehensive income, statement of changes in equity and statement of cash flows for the year ended on that date and the notes to the financial statements that include accounting policies and other explanatory information; and
- the performance information of the Privacy Commissioner on pages 25 to 34.

In our opinion:

- the financial statements of the Privacy Commissioner:
    - present fairly, in all material respects:
        - its financial position as at 30 June 2015;
        - its financial performance and cash flows for the year then ended; and
    - comply with generally accepted accounting practice in New Zealand and have been prepared in accordance with Public Benefit Entity Standards with reduced disclosure requirements.
- the performance information:
    - presents fairly, in all material respects, the Privacy Commissioner's performance for the year ended 30 June 2015, including:
        - for each class of reportable outputs:
            - its standards of performance achieved as compared with forecasts included in the statement of performance expectations for the financial year;

- its actual revenue and output expenses as compared with the forecasts included in the statement of performance expectations for the financial year;
- what has been achieved with the appropriation;
- the actual expenses or capital expenditure incurred compared with the appropriated or forecast expenses or capital expenditure; and

- complies with generally accepted accounting practice in New Zealand.

Our audit was completed on 21 October 2015. 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 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 the 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 the 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 the performance information. The procedures selected depend on our judgement, including our assessment of risks of material misstatement of the financial statements and the 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 performance information 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 performance information within the Privacy Commissioner's framework for reporting performance;
- the adequacy of the disclosures in the financial statements and the performance information; and
- the overall presentation of the financial statements and the performance information.

We did not examine every transaction, nor do we guarantee complete accuracy of the financial statements and the performance information. Also, we did not evaluate the security and controls over the electronic publication of the financial statements and the performance information.

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 performance information that:

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

The Privacy Commissioner's responsibilities arise from the Crown Entities Act 2004 and the Public Finance Act 1989.

The Privacy Commissioner is responsible for such internal control as it determines is necessary to enable the preparation of financial statements and 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 the performance information, whether in printed or electronic form.

Responsibilities of the Auditor

We are responsible for expressing an independent opinion on the financial statements and the performance information and reporting that opinion to you based on our audit. Our responsibility arises from the Public Audit Act 2001.

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.

Athol Graham
Audit New Zealand
On behalf of the Auditor-General
Auckland, New Zealand

STATEMENT OF PERFORMANCE

The Justice Sector has an aspirational outcome that all New Zealanders should expect to live in a safe and just society. This aspiration is supported by the Office as a Justice Sector Crown Entity. While the Office of the Privacy Commissioner is an Independent Crown entity and strongly maintains such independence, the work programme that it set out in its Statement of Intent and Statement of Performance Expectations, complements this aspiration and government priorities as a whole.

The Statement of Intent identified five strategic initiatives to support the Office's strategic objective of promoting and protecting individual privacy. The Statement of Performance Expectations identified four output classes to support these initiatives as illustrated below.

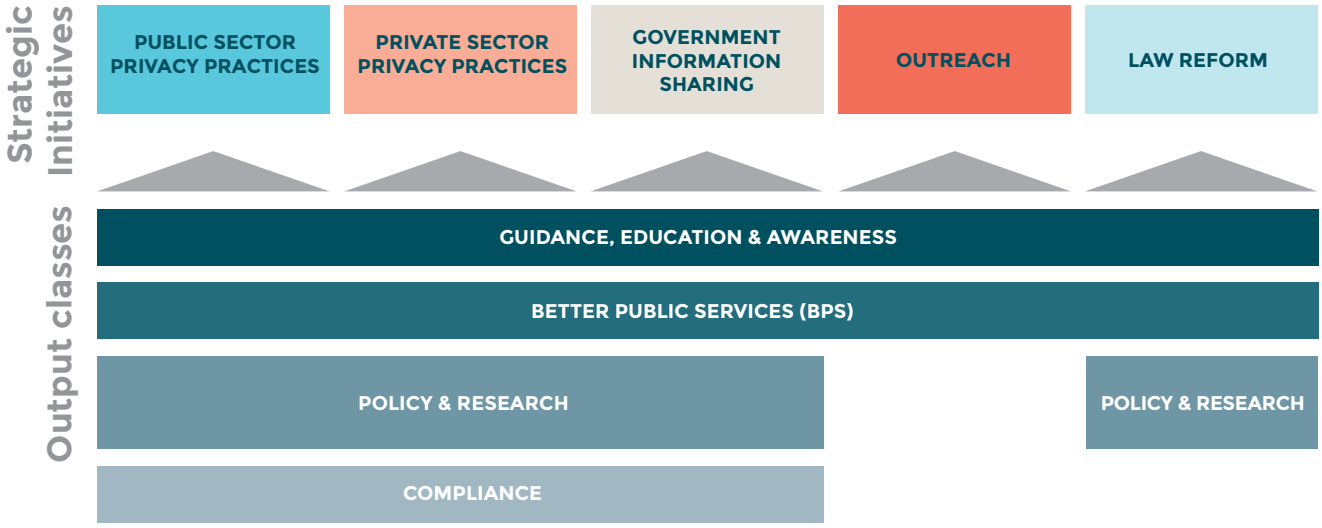

FIGURE ONE: THE RELATIONSHIP BETWEEN OUTPUT CLASSES AND STRATEGIC INITIATIVES

As noted in the Statement of Intent, the overall performance was to be measured through the service outputs and the detailed targets as set out further in this document. The following sets out a high level summary of the performance made by the office during the year against our strategic initiatives.

PERFORMANCE AGAINST STRATEGIC INTENTIONS/INITIATIVES

STRATEGIC INITIATIVE	WHAT WE EXPECTED TO ACHIEVE BY JUNE 2015	HOW WE HAVE PERFORMED
Public Sector privacy practices	Establish an active programme of engagement with the Government Chief Privacy Officer (GCIO) Identify capacity and capability needs of the Office Coordinated programme of activities established with GCIO Revise Privacy Impact Assessment handbook and guidance Data breach toolkits produced	Our engagement with the Government Chief Privacy Officer is positive and ongoing. We have established a programme of regular meetings between key staff in the offices and coordinate activities, particularly in relation to online training, guidance material and Privacy Week activities. The Privacy Impact Assessment handbook has been revised. An online training module is under development. The Data Safety toolkit was revised.
Private Sector privacy practices	Identify international initiatives which can be adopted to the New Zealand situation Programme of support to business Review of Credit Reporting Privacy Code	We liaise and coordinate with other data protection offices through international networks such as the Global Privacy Enforcement Network (GPEN) in the investigation and enforcement of privacy disputes. The Office released a Technology Strategy and work-plan. The strategy was developed after consultation with a number of predominantly private sector stakeholders in the business and technology fields. The online privacy statement generator, Priv-o-matic, was launched mid-year, and is aimed at SMEs. The proposal to review the Credit Reporting Code is under consideration.
Government information sharing	Process applications for information sharing in a timely manner Publish guidance for information sharing	Applications for AISAs were processed in a timely fashion. There are three approved agreements currently in place. New guidance for Approved Information Sharing Agreements (AISAs) was published and an online training module was released.
Outreach	Website upgrade scoped Review of naming policies and practices Create Privacy Commissioner's blog Website provides improved access to information and guidance Education review completed and comprehensive new programme launched	We have continued to actively review and upgrade our website through a variety of initiatives including the introduction of a blog, a Directory of Privacy Professionals, and a facility for secure online lodgement of complaints. The continuous improvement of our website is a high priority for the Office. Our Naming Policy was released after a process of consultation. The way the Office delivered education was reviewed in 2014 and the Office launched the first online privacy training modules during Privacy Week 2015. Three modules are currently available. Further modules are in development.
Law reform	Review and advise on policy associated with law reform Progress the law reforms through active contribution to the consultative and legislative process	We provided ongoing support and advice to the Ministry of Justice in relation to proposed privacy law reforms.

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	5,171	5,170
Other Revenue	301	342
Total Revenue	5,472	5,512

The operating grant is received as part of the Justice Advocacy, Advice and Promotion Services Appropriation within Vote Justice. This appropriation is intended to achieve the provision of justice advocacy, advice and promotion services through funding work across a number of Crown Entities including the Privacy Commissioner.

The amount above is equal to the original appropriation and there have not been any further appropriations made in the year. The amount received by the Privacy Commissioner equates to 22.6% of the total Justice Advocacy, Advice and Promotion Services Appropriation for 2014/15. The total expenses in the year are $4.871k as set out in the Cost of Service Statement below.

As set out in the 2014/15 Statement of Performance Expectations, the Privacy Commissioner committed to provide four output classes. The split of funds across these four output classes is set out below:

COST OF SERVICE STATEMENT FOR THE YEAR ENDED 30 JUNE 2015

	ACTUAL 2015 $000	BUDGET 2015 $000	ACTUAL 2014 $000
OUTPUT CLASS 1:			
Guidance, education and awareness			
Resources employed			
Revenue	716	692	1,204
Expenditure	585	727	1,217
Net Surplus(Deficit)	131	(35)	(13)
OUTPUT CLASS 2:			
Better Public Services			
Resources employed			
Revenue	896	896	371
Expenditure	747	896	374
Net Surplus(Deficit)	149	-	(3)
OUTPUT CLASS 3:			
Policy and research			
Resources employed			
Revenue	2,048	2,040	1,132
Expenditure	1,777	2,044	1,140
Net Surplus(Deficit)	271	(4)	(8)
OUTPUT CLASS 4:			
Compliance			
Resources employed			
Revenue	1,852	1,844	1,206
Expenditure	1,762	1,772	1,218
Net Surplus(Deficit)	90	72	(12)
TOTALS:			
Resources employed			
Revenue	5,512	5,472	3,913
Expenditure	4,871	5,439	3,949
Net Surplus(Deficit)	641	33	(36)

Note: the output classes were re-set during the drafting of the 2014/15 Statement of Performance Expectations. This resulted in a reduction from 6 to 4 output classes. The 2014 comparatives have therefore been amended accordingly whilst the totals have remained the same.

OUTPUT CLASS 1: GUIDANCE, EDUCATION AND AWARENESS

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.

Outreach is a major focus for the Office and includes a programme of workshops, public seminars, presentations and an active communications programme. During the 2014/15 year, the Office has developed new online privacy training modules which can be accessed at any time. This will help to extend the outreach potential for the Office.

Output Measures

Quantity			
MEASURE	**ESTIMATE**	**ACHIEVED 2014/15**	**ACHIEVED 2013/14**
Education workshops delivered	35[1]	Not achieved 26 During the year, the Office has developed and introduced new online training modules. To date, 3 modules have gone "live" and as at 31 July 2015 there were 2,760 people registered across the 3 modules. As a result of this, the number of face-to-face workshops delivered has reduced between 2013/14 and 2014/15.	39
Presentations at conferences / seminars	35	Achieved 96	62
Public enquiries received and answered	7,000[2]	Achieved 8,372 This represents all enquiries from members of the public.	8,765
Media enquiries received and answered	250	Achieved 273	286

1 This target was included within the Justice Advocacy, Advice and Promotion Services appropriation and was the same as the SPE target.

2 This target was included within the Justice Advocacy, Advice and Promotion Services appropriation. The SPE target above differs to the target of 6,000 per the appropriation. The appropriation clearly stated that measures "may be subject to change".

Quality			
MEASURE	**ESTIMATE**	**ACHIEVED 2014/15**	**ACHIEVED 2013/14**
Evaluations show that at least of 90% of respondents are satisfied with the overall effectiveness of the workshops they attended	90%[3]	97%	89%
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 Privacy Commissioner, and additional resources to support compliance with the Act.	Achieved	Achieved	Achieved
Guidance materials produced by the Privacy Commissioner meet the 'Plain English Writing Standard.'	Achieved	Partially achieved The office contracted with Write Limited to review a selection (7 documents) of guidance materials produced during the year. Each document was assessed against the 10 elements of the Plain English standard. The review showed a generally good standard across the documents, but also identified some areas for improvement. The Office met with Write Limited to discuss the detail of the review and suggested improvements.	Not reported – new measure

Timeliness			
MEASURE	**ESTIMATE**	**ACHIEVED 2014/15**	**ACHIEVED 2013//14**
Respond to 90% of 0800 line enquiries within one working day	90%	Achieved 99%	94%
Guidance materials are produced within agreed timelines	Achieved	Substantially Achieved Guidance materials were produced in a timely manner during the year. However, one major piece of guidance fell outside of the Office's expectations for timely delivery.	Not reported – new measure

OUTPUT CLASS 2: POLICY AND RESEARCH

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 privacy practices and information handling by government and business is a major threat to New Zealanders' privacy.

The Office actively comments and responds on legislative, policy or administrative proposals that impact on privacy so as to ensure that the requirements of the Privacy Act are being taken into account. Active involvement in international fora also takes place which provides the Privacy Commissioner with the ability to identify and respond to emerging issues in a timely manner.

3 This target was included within the Justice Advocacy, Advice and Promotion Services appropriation and was the same as the SPE target.

Output Measures

Quantity			
MEASURE	**ESTIMATE**	**ACHIEVED 2014/15**	**ACHIEVED 2013/14**
New policy files opened during the year	80	Achieved – 114 new policy files opened and worked on during the year.	81
Identifiable progress in international efforts in which we are engaged to enhance cooperation and interoperability between privacy laws across trading partners	Achieved	Achieved At its January 2015 meeting, APEC[4] Data Privacy Subgroup approved a paper prepared by the Office recommending updates to the APEC Privacy Framework. These were based on the 2013 reforms of the OECD[5] Privacy Guidelines and the alignment will enhance interoperability of privacy frameworks across two major groups of trading nations. Since October 2014, the Office has provided the Chair and Secretariat to the Executive Committee of the ICDPPC[6] as well as being the Convenor of the Strategic Direction Working Group. In these capacities the Office has worked to create capacity for the Conference to perform its objectives of advancing cooperation. Two key achievements were to build a permanent website to facilitate its work (launched April 2015) and designing, approving and operating a system for selecting future conference hosts with an earlier lead time to put the conference on a firm footing (process approved October 2014, process run for first time from December 2014 onward).	Not reported – new measure
Cross-border enforcement laws and practices in place	Achieved	Achieved Global Cross Border Enforcement Cooperation Arrangement adopted by ICDPPC as a means to facilitate cross-border cooperation. GPEN[7] Alerts system will provide a secure means for privacy enforcement authorities to communicate details of investigations having cross-border implications. The system has been developed over several years with close Office involvement and moved very close to completion with approval of final documentation. The Office agreed to participate in beta testing which commenced shortly after the end of the year.	Not reported – new measure
Maintain close working relationship with Ministry of Justice officials on the content and progress of the Law reform	Achieved	Achieved The Office has worked proactively with the Ministry during the year in relation to the Law Reform.	Not reported – new measure

Quality			
MEASURE	**ESTIMATE**	**ACHIEVED 2014/15**	**ACHIEVED 2013/14**
Survey of recipients of policy advice indicate that at least 70% are satisfied with the service they received from the Privacy Commissioner	Achieved	Achieved – 96%	Not reported – new measure
Our participation in the law reform process is valued by stakeholders	Achieved	Achieved Based on feedback received through the annual stakeholder survey carried out.	Not reported – new measure

4 Asia-Pacific Economic Cooperation (APEC)

5 Organisation of Economic Co-operation and Development (OECD)

6 International Conference of Data Protection and Privacy Commissioners (ICDPPC)

7 Global Privacy Enforcement Network (GPEN)

Timeliness			
MEASURE	ESTIMATE	ACHIEVED 2014/15	ACHIEVED 2013/14
Advice on proposals provided within agreed timeframes	90%	Achieved – 100%	84%
Requests for input into law reform is made available within agreed timelines	90%	Achieved – 100%	Not reported – new measure

OUTPUT CLASS 3: BETTER PUBLIC SERVICES

Why is this important?

Trust in government is a cornerstone of Better Public Services, and is an asset to business that, once lost, is difficult to regain.

The public attitude survey, undertaken on behalf of the Office by UMR Research in 2014, identified high levels of concern amongst New Zealanders about the sharing of personal information with other government agencies.

Securing personal data has become a greater challenge. Individuals are exposed to increased potential harms including the risk of identity theft. Data breaches are occurring more frequently and data breach notification is an increasingly important element of the Office, along with raising awareness of the need to have effective information risk management strategies in place across organisations that collect, share or use personal information.

Output Measures

Quantity			
MEASURE	ESTIMATE	ACHIEVED 2014/15	ACHIEVED 2013/14
Information matching programmes monitored	52[8]	Achieved 57 There are 56 current programmes and 1 programme which ceased in August 2014.	56
New information sharing or matching programmes assessed	10	Not achieved. 1 new information sharing proposal was assessed during the year and 1 existing information sharing programme was amended.	3
Toolkit produced for government agencies preparing to implement new information sharing programmes	Achieved	Achieved The AISA (Approved Information Sharing Agreements) guidance was produced during the year.	Not reported – new measure
Complaints able to be made online through the Privacy Commissioner website	Achieved	Achieved During the year, the Office enhanced its website to enable complaints to be lodged online. So far this has proved to be successful with approximately 28% of complaints being lodged in this way since it was launched.	Not reported – new measure
An active programme of engagement with the Government Chief Privacy Officer (GCPO) to improve the handling of personal information within the public sector	Achieved	Achieved There is an agreed Memorandum of Understanding (MoU) in place and discussions have taken place between the two parties during the year.	Not reported – new measure

8 This target was included within the Justice Advocacy, Advice and Promotion Services appropriation and was the same as the SPE target.

Quality			
MEASURE	**ESTIMATE**	**ACHIEVED 2014/15**	**ACHIEVED 2013/14**
All statutory obligations to report on information matching met	100%	Achieved 100% The statutorily required information matching reports (as set out in s105 and s106 of the Privacy Act 1993) have been completed as required.	4 information matches were commenced in 2013/14. They remained under progress for completion and reporting in 2014/15.
60% of recommendations from formal review of information sharing or matching programmes have been acted upon within 30 working days of the date of the review report being received	Achieved	Achieved There has only been one formal recommendation during the year as a result of a review carried out as per s106. Due to the nature of the recommendation (which involved reviewing legislation), action will be required within 2 years.	Not reported – new measure
A trend of reducing concern about government agencies sharing personal information	Achieved	Not measured in the year. The survey used to assess this was last undertaken in 2014. The next survey is due to be carried out in 2016.	Not reported – new measure

Timelines			
MEASURE	**ESTIMATE**	**ACHIEVED 2014/15**	**ACHIEVED 2013/14**
Statutory timelines for reporting on information matching met	100%	Achieved 100% The s105 requirements have been met as set out in this Annual Report. In terms of s106, there were 4 such reports completed in the year.	Achieved.
Percentage of responses to requests to review information sharing agreements provided within agreed timeframes	90%	Achieved – 94%	100%

OUTPUT CLASS 4: COMPLIANCE

Why is this important?

Personal data is increasingly a core asset for modern business operations and is essential to effective government administration and the delivery of services. The growing value of personal data increases the risk that data will be used in ways that neither the organisation nor the individual anticipated when the data was collected.

Through a process of private and public sector consultation the Office develops codes to either modify the information privacy principles or prescribe how the information privacy principles are to be applied or complied with in a particular industry or context.

To effectively address growing concerns or queries from New Zealanders, the office provides an independent responsive complaints and investigation process.

Output Measures

Quantity			
MEASURE	**ESTIMATE**	**ACHIEVED 2014/15**	**ACHIEVED 2013/14**
Number of complaints received	800[9]	Achieved – 835 new complaints received	725
Number of current complaints processed to completion or settled or discontinued	800[10]	Achieved – 827 complaints files closed	702

Quality			
MEASURE	**ESTIMATE**	**ACHIEVED 2014/15**	**ACHIEVED 2013/14**
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%[11]	Not achieved – the overall satisfaction rating for the year was 53%. There were a total of 293 responses to the survey during the year which represents 34% of the total complaints closed. As in prior years, the survey asks for overall satisfaction with the quality of service provided rather than satisfaction with the outcome. 29% of complainants and 84% of respondents reported being satisfied with the overall quality of the service provided. Both of these are lower than the corresponding results in 2014 (39% for complainants and 87% for respondents). This survey will be an area of focus over next year and work has already commenced in this area.	60%
Of the complaints processed, 30% are closed by settlement between the parties	Achieved	Achieved – 44% This is a significant achievement for the Office and is an increase of 12% on the prior year and 14% on the target.	32%
Amendments to Codes of Practice meet all statutory requirements	100%	Achieved The statutory requirements of Part 6 of the Privacy Act were met. Two amendments to existing codes were issued during the year. The amendments were: i. Justice Sector Unique Identifier Code Amendment No. 3. ii. Credit Reporting Privacy Code 2004 Amendment No 9.	Not applicable as no amendments were issued in the year.

9 This target was included within the Justice Advocacy, Advice and Promotion Services appropriation. The SPE target above differs to the target of 900 per the appropriation. The appropriation clearly stated that measures "may be subject to change".

10 This target was included within the Justice Advocacy, Advice and Promotion Services appropriation. The SPE target above differs to the target of 900 per the appropriation. The appropriation clearly stated that measures "may be subject to change".

11 This target was included within the Justice Advocacy, Advice and Promotion Services appropriation and was the same as the SPE target.

Number of complaints received	800[9]	Achieved – 835 new complaints received	725
An external review of a sample of complaints investigations rates 70% as 3.5 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 - 57% An independent auditor was engaged to perform a review of 30 files selected at random. Whilst the auditor advised the overall standard of the files was very high, with the investigators displaying high levels of professionalism, the target was not achieved with only 17 of the files scoring 3.5 or better. As direct comparisons to the prior year, 43% of files audited were rated 4 out of 5 or better compared to the 29% in 2014. The key factors affecting this result were timeliness and procedural clarity. Work is underway to addressing these issues, including the development of a procedure manual.	29% rated 4 out of 5 or better and 91% rated 3.75 or better (measure amended for current SPE)

Timelines			
MEASURE	**ESTIMATE**	**ACHIEVED 2014/15**	**ACHIEVED 2013/14**
Complaints received are acknowledged within 5 days of receipt	100%	Not achieved - 87% This represents complaints where there was a formal acknowledgement letter sent out within 5 days of receipt. The search for "acknowledgment letters" in our complaints management system does not capture the work that is done by enquiries officers and investigators at an early stage after receiving a new complaint, referring it back to the agency involved, gathering more information, or undertaking phone based resolution and negotiation. The result is therefore potentially higher than the 87% being reported. For the next financial year, the office will develop strategies to record first contacts and acknowledgments in a more accurate way rather than just by formal acknowledgement letters.	Not reported – new measure
80% of complaints are completed, settled or discontinued within nine months of receipt	85%[12]	Achieved 85% 702 out of the 827 files closed during the year were closed within 9 months of them being received.	88%
Review of the operation of Credit Reporting Code commenced	Achieved	Commenced Preliminary work to review the operation of aspects of the Credit Reporting Privacy Code commenced from December 2014 onward. A review of the operation of the amendments No 4 and 5 was scheduled to commence "as soon as practicable" after 1 April 2015, being 3 years after those amendments, which authorised positive reporting, commenced. As a preliminary step in the work of such a review enquiries were made of the national credit reporters (December 2014) which established that the slower than expected implementation of positive reporting supported a delay of an active review programme beyond the end of the financial year.	Not reported – new measure

12 This target was included within the Justice Advocacy, Advice and Promotion Services appropriation. The SPE target above differs to the target of 80% per the appropriation. The appropriation clearly stated that measures "may be subject to change".

STATEMENT OF ACCOUNTING POLICIES

FOR THE YEAR ENDED 30 JUNE 2015

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 financial reporting purposes.

The financial statements for the Privacy Commissioner are for the year ended 30 June 2015, and were approved by the Commissioner on 21 October 2015. The financial statements cannot be altered after they have been authorised for issue.

Basis of preparation

The financial statements have been prepared on a going concern basis, and the accounting policies have been applied consistently throughout the period.

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 have been prepared in accordance with Tier 2 PBE accounting standards. The Tier 2 criteria have been met as expenditure is less than $30m and the Privacy Commissioner is not publicly accountable (as defined in XRB A1 Accounting Standards Framework).

These financial statements comply with PBE accounting standards.

These financial statements are the first financial statements presented in accordance with the new PBE accounting standards. The material adjustments (where applicable) arising on transition to the new PBE accounting standards are explained in note 24.

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 revenue and expenses, 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.

Cost allocation

The Privacy Commissioner has determined the costs of outputs using a cost allocation system as outlined below.

Direct Costs are those costs directly attributed to an output. These costs are therefore charged directly to the outputs.

Indirect costs are those costs that cannot be identified in an economically feasible manner with a specific output. Personnel costs are charged based on % of time spent in relation to each output area. Other indirect costs are allocated based on the proportion of staff costs for each output area.

There have been no substantial changes to the cost allocation methodology since the date of the last audited financial statements.

Revenue

The specific accounting policies for significant revenue items are explained below:

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 and Statement of Performance Expectations.

The Privacy Commissioner considers there are no conditions attached to the funding and it is recognised as revenue at the point of entitlement.

The fair value of revenue from the Crown has been determined to be equivalent to the amounts due in the funding arrangements.

Other grants

Non-government grants are recognised as revenue when they become receivable unless there is an obligation in substance 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 treated as exchange revenue and 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

Short term debtors and receivables are recorded at their face value, less any provisions for impairment.

A receivable is considered impaired when there is evidence that the Privacy Commissioner will not be able to collect the amount due according to the terms of the receivable. Significant financial difficulties, 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 carrying amount of the receivable and the present value of the amounts expected to be collected.

Inventories

Inventories held for distribution, or consumption in the provision of services, that are not issued on a commercial basis are measured at cost.

Inventories held for sale or use in the provision 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 revenue and expenses 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 through a non-exchange transaction (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 revenue and expenses 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 measured at their face value.

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 Kiwi Saver 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 revenue and expenses.

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 2015:

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.

STATEMENT OF COMPREHENSIVE REVENUE AND EXPENSES

FOR THE YEAR ENDED 30 JUNE 2015

	NOTE	ACTUAL 2015 $000	BUDGET 2015 $000	ACTUAL 2014 $000
Revenue				
Crown Revenue	2	5,170	5,171	3,584
Other Revenue	3	274	261	297
Interest		68	40	32
Total Income		5,512	5,472	3,913
Expenditure				
Promotion	4	109	156	111
Audit Fees		28	25	27
Depreciation and Amortisation	1, 10, 11	144	170	100
Rental Expense		383	413	352
Operating Expenses		669	551	451
Contract Services		250	300	99
Staff Expenses	5	3,288	3,824	2,809
Total Expenditure		4,871	5,439	3,949
Surplus/(Deficit)		641	33	(36)
Other comprehensive revenue and expenses		-	-	-
Total Comprehensive Revenue and expenses		**641**	**33**	**(36)**

STATEMENT OF CHANGES IN EQUITY

FOR THE YEAR ENDED 30 JUNE 2015

	NOTE	ACTUAL 2015 $000	BUDGET 2015 $000	ACTUAL 2014 $000
Total Equity at the start of the year		756	842	792
Total comprehensive revenue and expenses for the year		**641**	**33**	**(36)**
Total Equity at the end of the year	**6**	**1,397**	**875**	**756**

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 2015

	NOTE	ACTUAL 2015 $000	BUDGET 2015 $000	ACTUAL 2014 $000
Public Equity				
General funds	6	1,397	875	756
Total public equity		1,397	875	756
Current assets				
Cash & cash equivalents	7	1,052	925	798
Receivables	8	173	8	2
Inventory	9	23	8	11
Prepayments	8	17	11	22
Total Current Assets		1,265	953	833
Non-current assets				
Property, Plant & Equipment	10	539	151	149
Intangible assets	11	37	-	64
Total non-current assets		576	151	213
Total assets		**1,841**	1,104	1,046
Current liabilities				
Payables	12	215	120	167
Employee entitlements	14	138	109	122
Total current liabilities		353	229	289
Non-current liabilities				
Lease incentive	13	91	-	-
Total non-current liabilities		91	-	-
Total Liabi lities		**444**	229	289
Net assets		**1,397**	875	756

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

STATEMENT OF CASH FLOWS

FOR THE YEAR ENDED 30 JUNE 2015

	ACTUAL 2015 $000	BUDGET 2015 $000	ACTUAL 2014 $000
Cash flows from operating activities			
Cash was provided from:			
Supply of outputs to the Crown	5,376	5,171	3,790
Revenues from services provided	69	261	96
Interest received	67	40	32
Cash was applied to:			
Payment to suppliers	1,144	1,719	904
Payments to employees	3,521	3,550	2,895
Net Goods and Services tax	71	(8)	(44)
Net cash flows from operating activities	**776**	**211**	**163**
Cash flows from investing activities			
Cash was applied to:			
Purchase of Property Plant and Equipment	522	110	27
Purchase of Intangible Assets	-	-	34
Net cash flows from investing activities			
Net increase (decrease) in cash held	254	101	102
Plus opening cash	798	824	696
Closing cash balance	1,052	925	798
Cash and bank	**1,052**	**925**	**798**
Closing cash balance	**1,052**	**925**	**798**

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 2015

NOTE 1: TOTAL COMPREHENSIVE REVENUE AND EXPENSES

	ACTUAL 2015 $000	ACTUAL 2014 $000
The total comprehensive revenue and expenses is after charging for:		
Fees paid to auditors		
External audit		-
Current Year	28	27
Prior Year	-	27
Depreciation:		
Furniture & Fittings	43	17
Computer Equipment	62	54
Office Equipment	12	7
Total Depreciation for the year	**117**	**78**
Amortisation of Intangibles	27	22
Rental expense on operating leases	383	352
Loss on disposal of assets	16	-

Explanation of major variances

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

Statement of Comprehensive Income

The year-end surplus is significantly higher than the budgeted surplus which is primarily due to the following:

Operating expenses (up $118k on budget)

There has been increased expenditure against budget in the areas of computer maintenance and travel. These accounted for $82k of the increase. Travel cost increases resulted due to the additional staff towards the end of the year.

Staff Expenses (down $536k on budget)

The budget included the addition of new posts mainly within the Policy and Operations and Corporate Services Teams. These posts either remained unfilled at the year-end or were filled later on in the year leading to a significantly lower salary cost than originally budgeted.

Marketing Costs (down $47k on budget)

The decreased expenditure is as a result of lower than expected advertisement related costs. The costs, whilst down on expectation, were in line with prior years.

Contract Services (down $51k on budget)

The Office has significantly increased its expenditure on contract services from the prior year but expenditure still fell below budget. The legal and policy area had the most significant fall against budget ($50k).

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 (2014: $nil).

NOTE 3: OTHER REVENUE

	ACTUAL 2015 $000	ACTUAL 2014 $000
Other grants received	206	206
Rental income from property sub-leases	25	25
Privacy Forum	-	25
Seminars & Workshops	43	38
Other	-	2
Total other revenue	**274**	**296**

NOTE 4: PROMOTION EXPENSES

	ACTUAL 2015 $000	ACTUAL 2014 $000
Website development expenses	91	41
Publications	-	2
Privacy Forum	6	8
Other marketing expenses	12	60
Total marketing expenses	**109**	**111**

NOTE 5: STAFF EXPENSES

	ACTUAL 2015 $000	ACTUAL 2014 $000
Salaries and wages	3,040	2,732
Employer contributions to defined contribution plans	86	34
Other Staff expenses	146	33
Increase/(decrease) in employee entitlements	16	10
Total Staff Expenses	**3,288**	**2,809**

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

The prior year note included "Other contracted services". This is now shown separately on the face of the Statement of Comprehensive Revenue and Expenses rather than being included within Staff Expenses.

NOTE 6: GENERAL FUNDS

	ACTUAL 2015 $000	ACTUAL 2014 $000
Opening balance	756	792
Net (deficit) / surplus	641	(36)
Closing balance	**1,397**	**756**

NOTE 7: CASH AND CASH EQUIVALENTS

	ACTUAL 2015 $000	ACTUAL 2014 $000
Cash on hand and at bank	86	51
Cash equivalents – on call account	966	747
Total cash and cash equivalents	**1,052**	**798**

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

NOTE 8: RECEIVABLES

	ACTUAL 2015 $000	ACTUAL 2014 $000
Receivables	173	2
Prepayments	17	22
Total	**190**	**24**
Total receivables comprise:		
Receivables in relation to lease incentive (exchange transaction)	120	
GST receivables (exchange transaction)	52	
Other receivables	1	2
Total	**173**	**2**

The carrying value of receivables approximates their fair value. The receivables balance includes $120K due in relation to the lease incentive on the new Wellington office.

The carrying amount of receivables that would otherwise be past due, but not impaired, whose terms have been renegotiated is $NIL (2014: $NIL).

NOTE 9: INVENTORIES

	ACTUAL 2015 $000	ACTUAL 2014 $000
Publications held for sale	9	11
Publications held for distribution	14	-
Total Inventories	**23**	**11**

There have been no write-down of inventories held for distribution or reversals of write-downs (2014 $NIL).

No inventories are pledged as security for liabilities (2014: $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 2013	415	248	71	734
Additions	1	10	17	28
Disposals				
Balance at 30 June 2014	**416**	**258**	**88**	**762**
Balance at 1 July 2014	**416**	**258**	**88**	**762**
Additions	419	94	9	522
Disposals	(120)	(47)	(38)	(205)
Balance at 30 June 2015	**715**	**305**	**59**	**1,079**
Accumulated depreciation and impairment losses				
Balance at 1 July 2013	371	116	47	534
Depreciation expense	17	54	7	78
Disposals				
Balance at 30 June 2014	**388**	**170**	**54**	**612**
Balance at 1 July 2014	**388**	**170**	**54**	**612**
Depreciation expense	43	62	12	117
Elimination on disposal	(108)	(47)	(34)	(189)
Balance at 30 June 2015	**323**	**185**	**32**	**540**
Carrying amounts				
At 1 July 2014	**28**	**88**	**34**	**150**
At 30 June 2015	**392**	**120**	**27**	**539**

NOTE 11: INTANGIBLE ASSETS

Movements for each class of intangible asset are as follows:

	ACQUIRED SOFTWARE 2015 $000
Cost	
Balance at 1 July 2013	73
Additions	33
Balance at 30 June 2014	106
Balance at 1 July 2014	106
Additions	-
Balance at 30 June 2015	106
Accumulated amortisation and impairment losses	
Balance at 1 July 2013	21
Amortisation expense	21
Balance at 30 June 2014	42
Balance at 1 July 2014	42
Amortisation expense	27
Balance at 30 June 2015	69
Carrying amounts	
At 1 July 2013	52
At 30 June and 1 July 2014	64
At 30 June 2015	**37**

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: PAYABLES

	ACTUAL 2015 $000	ACTUAL 2014 $000
Payables under exchange transactions		
Creditors	110	73
Accrued expenses	85	76
Lease incentive	20	-
Total payables under exchange transactions	215	149
Payables under non-exchange transactions		
Other payables (GST)	0	18
Total payables under non-exchange transactions	0	18
Total creditors and other payables	**215**	**167**

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: NON-CURRENT LIABILITIES

	ACTUAL 2015 $000	ACTUAL 2014 $000
Lease incentive	91	-
Total non-current liabilities	91	-

Lease incentive for the Wellington office at level 8, 109-111 Featherston Street for the period 23 February 2015 to 22 February 2021 (6 year lease).

NOTE 14: EMPLOYEE ENTITLEMENTS

	ACTUAL 2015 $000	ACTUAL 2014 $000
Current employee entitlements are represented by:		
Accrued salaries and wages	27	13
Annual leave	111	109
Total current portion	**138**	**122**
Current	138	122
Non-current	-	-
Total employee entitlements	**138**	**122**

NOTE 15: CAPITAL COMMITMENTS AND OPERATING LEASES

Capital commitments

The Privacy Commissioner has capital commitments of $nil for the year 2014/15. (2014: $47,050).

Operating leases

	ACTUAL 2015 $000	ACTUAL 2014 $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	365	345
Later than one year and not later than five years	1,346	614
Later than five years	159	11

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. During the year the Wellington office moved floors and a new 6 year lease was entered into. A lease incentive was offered as part of the negotiation. This has been accounted for in line with PBE IPSAS 13 Leases (see Note 12 and 13). The property In Auckland has been sublet in part, due to it being surplus to requirements during the 2014/15 year. Notice has been given to the current tenants and this space will be taken back during the 2015/16 year. The lease on the Auckland premises will expire on 31 July 2019.

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 (2014: $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.

Related part disclosures have not been made for transactions with related parties that are within a normal supplier or client/recipient relationship on terms and conditions no more or less favourable than those that

it is reasonable to expect the Privacy Commissioner would have adopted in dealing with the party at arm's length in the same circumstances. Further, transactions with other government agencies (for example, Government departments and Crown entities) are not disclosed as related parties transactions when they are consistent with the normal operating arrangements between government agencies and undertaken on the normal terms and conditions for such transactions.

There were no other related party transactions.

Key management personnel compensation

	ACTUAL 2015 $000	ACTUAL 2014 $000
Total Salaries and other short-term employee benefits	1,060	1,123
Full-time equivalent members	5.9	5.8

Key management personnel include all Senior Managers and the Privacy Commissioner who together comprise the Senior Leadership Team (SLT). There have been some changes in the composition of the SLT during the year with some members leaving and new members joining but the number of overall members has remained relatively consistent.

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 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 their annual reports. The information reported is the number of employees receiving total remuneration of $100,000 or more per annum. In compliance, the table below has been produced, which is in $10,000 bands to preserve the privacy of individuals.

TOTAL REMUNERATION AND BENEFITS	NUMBER OF EMPLOYEES	
	ACTUAL 2015	ACTUAL 2014
$100,000 - $109,999	2	
$110,000 - $119,999		2
$120,000 - $129,999	1	
$130,000 - $139,999		
$140,000 - $149,999		1
$150,000 - $159,999	1	2
$160,000 - $169,999	1	
$170,000 - $179,999	1	1
$300,000-$309,999	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 2014 to 30 June 2015. John Edwards was appointed Privacy Commissioner to replace Marie Shroff effective on 17 February 2014.

NAME	POSITION	AMOUNT 2015	AMOUNT 2014
John Edwards	Privacy Commissioner (From 17 February 2014)	300,700	$102,783
Marie Shroff	Privacy Commissioner (1 July 2013 to 16 February 2014)	-	$287,812

The amount paid to Marie Shroff in 2014 included retirement leave due in accordance with her employment provisions, at the cessation of her term as Privacy Commissioner.

NOTE 20: CESSATION PAYMENTS

No redundancy payments were made in the year. (2014: $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 carrying amounts of financial assets and liabilities in each of the financial instrument categories are as follows:

	2015 $000	2014 $000
FINANCIAL ASSETS		
Loans and Receivables		
Cash and cash equivalents	1,052	798
Receivables (excluding prepayments and taxes receivables)	122	2
Total loans and receivables	**1,174**	800
FINANCIAL LIABILITIES		
Financial liabilities at amortised cost		
Payables (excluding income in advance, taxes payable, grants received subject to conditions and lease incentive)	195	167
Total financial liabilities at amortised cost	**195**	167

NOTE 24: ADJUSTMENTS ARISING ON TRANSITION TO THE NEW PBE ACCOUNTING STANDARDS

Reclassification adjustments

There have been no reclassifications on the face of the financial statements in adopting the new PBE accounting standards.

There have been minor amendments to certain notes for payables and receivables to classify balances depending on whether they relate to an exchange or non-exchange transaction. See notes 8 and 12.

Recognition and measurement adjustments

There have been no material recognition and measurement adjustments as a result of the adoption of the new PBE accounting standards.

Appendix A – Processes and services

Investigations

Our investigations team forms the dispute resolution side of the Office's functions. The team receives privacy complaints from individuals (complainants) about agencies (respondents). These complaints can be about a number of different issues, such as an improper disclosure of information, improper collection, or refusal to reveal or amend the information agencies hold about individuals.

Agencies are usually not liable for privacy breaches unless the complainant can demonstrate an 'interference with privacy'. This is a privacy breach that causes harm – such as negative physical, emotional or financial effects from the breach. However, a complainant does not have to demonstrate harm in cases involving the access to or correction of their personal information.

If a situation is covered by the Privacy Act, we may begin an investigation. During the course of an investigation we will often gather information about the events that took place and the actions of the respondent agency. We will often ask the complainant to provide some detail about the harm they feel they have suffered. We try to identify options for a resolution at every point in the process.

When there has been an interference with privacy and the two parties cannot settle the case, we have the option of referring the case to the Director of Human Rights Proceedings, who may choose to bring the case to the Human Rights Review Tribunal. We do not always refer cases. We will be likely to refer cases that are particularly serious or where there are new matters of law that need to be decided by the courts.

If we choose not to refer a case to the Director, or the Director chooses not to proceed with a case that we refer, the complainant still has the option of taking the respondent to the Tribunal on their own. A complainant cannot bring a case until our office has investigated their complaint.

During the course of an investigation we can compel agencies to produce documents, and we can compel agencies to meet with complainants. We cannot compel complainants or respondents to accept settlement terms and we cannot award damages.

Policy

Our policy team provides advice for a range of organisations on the privacy risks of various initiatives. We also offer advice to help organisations mitigate privacy risks.

Our advice is sometimes solicited from agencies that are looking to amend internal policy, and we sometimes proactively provide advice on upcoming legislation. This is generally in the form of submissions to Select Committees, but we also provide input into Cabinet papers and may brief Cabinet in person.

A significant portion of our policy work involves proposals to improve public service delivery by sharing information. We consult on these agreements and highlight potential risks, much like we do for other policy projects.

Finally, we engage with the private sector to consult on a variety of projects, such as privacy impact assessments. This is a growing area as more private sector organisations manage their privacy risk by engaging with our team early in technology deployment projects.

Information matching

Information matching involves the comparison of one set of records with another, generally to find records in both sets that belong to the same person.

Information matching raises a number of privacy issues, such as the potential to disclose incorrect or out of date information or the potential to supplant human judgement. For this reason, the Privacy Act regulates information matching in the public sector.

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.

Communications and outreach

Our communications team works to raise privacy awareness. We work through a significant number of channels, producing material such as:

- speeches and presentations for the Commissioner
- media releases and advisories
- blog posts and social media updates
- case notes
- the "Privacy Digest" newsletter

We also produce guidance to assist with the objective of 'making privacy easy.' A key component of this guidance is our online training. We have worked with education experts to build online courses about various aspects of privacy. This is in addition to written guidance. Finally, we respond to enquiries – both from journalists in traditional media and from the public in social media.

Appendix B – information matching programme compliance

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 a programme's compliance according to one of 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.

ACCIDENT COMPENSATION ACT 2001, S.246	
	COMPLIANCE
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)	
	COMPLIANCE
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	
	COMPLIANCE
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.	✓

BIRTHS, DEATHS AND MARRIAGES ACT 1995, S.78A	COMPLIANCE
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.	✓
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 disclosure 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.	✓
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 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.	✓
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.	✓
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 extraction date. The death details include the full name (current and at birth), gender, date and place of birth, date of death, home address and death registration number.	✓
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.	✓
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 of birth and place of birth, birth registration number and full name and date of birth of both mother and father.	✓
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: The content of the section 103 letter sent for this programme did not fully meet statutory requirements. The letter – which goes to individuals affected by adverse action as a result of the information matching – did not state that individuals have five working days to show why action should not be taken. MSD updated the template wording to meet requirements in July 2015.	X
CITIZENSHIP ACT 1977, S.26A	
	COMPLIANCE
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 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	
	COMPLIANCE
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.	✓
CORRECTIONS ACT 2004, S.181	
	COMPLIANCE
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	
	COMPLIANCE
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.	✓
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	
	COMPLIANCE
30. MoE/Teachers' Council Registration To ensure teachers are correctly registered (Teachers Council) and paid correctly (MoE). 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	
	COMPLIANCE
31. Educational Institutions/MSD (Study Link) Loans and Allowances To verify student enrolment information to confirm entitlement to allowances and loans. MSD StudyLink 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.	✓
EDUCATION ACT 1989, S.307D	
	COMPLIANCE
32. MoE/MSD (Study Link) 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: When the file is moved within StudyLink's Student Allowance and Loan system a copy is left behind on a staging system that the file is moved across. This was a potential security issue. MSD will do some system testing and then manually delete these copies until an automated deletion function can be set up.	X

ELECTORAL ACT 1993, S.263A AND S.263B	COMPLIANCE
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 (EC): Citizenship provides full names, dates of birth and residential addresses 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: INZ provides full names (including aliases), date of birth, address and permit expiry date. The type of permit can be identified because five separate files are received, each relating to a different permit type.	✓
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 EC: NZTA provides full names, dates of birth and addresses 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 EC: MSD provides full names, dates of birth and addresses 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.	✓
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 EC: NZTA provides the full names, dates of birth and addresses 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 EC: Passports provides full names, dates of birth and residential addresses of passport holders aged 17 years and over.	✓

ELECTRONIC IDENTITY VERIFICATION ACT 2012, S.39	
	COMPLIANCE
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. Births disclosure to IVS: Name, 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: Name, gender, date of birth, place of birth, date of death, place of death and age at death. Marriages disclosure to IVS: Name, date of birth, date of marriage, registration number, country of birth, gender, place of marriage, spouse's names. Citizenship disclosure to IVS: Name, gender, birth date, birth place, photograph, citizenship person identifier, citizenship certificate number, certificate type and certificate status. Passports disclosure to IVS: Name, 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.	✓

HOUSING RESTRUCTURING AND TENANCY MATTERS ACT 1992, S.68	
	COMPLIANCE
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. This programme ceased operating in August 2014 as responsibility for administering income-related rents has transferred from HNZ to MSD.	✓

IMMIGRATION ACT 2009, S.295	
	COMPLIANCE
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).	✓

IMMIGRATION ACT 2009, S.300	
	COMPLIANCE
42. INZ/MoH Publically Funded Health Eligibility To enable MoH to determine an individual's: • eligibility for access to publically funded health and disability support services; or • liability to pay for publically 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, visa 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.	✓

MOTOR VEHICLE SALES ACT 2003, SS.120 AND 121	
	COMPLIANCE
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. Minor Technical Issues: Two issues were identified in an online transfer audit. Firstly, MBIE stopped using the approved SEEMail email system for transfers with Customs when a new email security classification system was introduced. Secondly, data received from Customs was found to incorrectly include details of individuals who have imported three vehicles when the purpose of the programme is to identify individuals that import more than three vehicles as specified in the Technical Standards Report. This was outside the scope of the agreement. Both issues have been resolved.	X

MOTOR VEHICLE SALES ACT 2003, SS.122 AND 123	
	COMPLIANCE
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. Minor Technical Issue: Additional data about trailers and agricultural vehicles not specified in the Technical Standards Report was being provided to MBIE. This information was outside the scope of the information matching agreement. This issue has been resolved.	X

SOCIAL SECURITY ACT 1964, S.126A	
	COMPLIANCE
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 and work phone numbers and the unique identifier originally provided by Justice.	✓

SOCIAL SECURITY ACT 1964, S.126AC	
	COMPLIANCE
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.	✓

SOCIAL WELFARE (RECIPROCITY AGREEMENTS, AND NEW ZEALAND ARTIFICIAL LIMB SERVICE) ACT 1990, SS.19C AND 19D AND SOCIAL WELFARE (RECIPROCITY WITH AUSTRALIA) ORDER 2002, ARTICLE 18	
	COMPLIANCE
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.	✓

SOCIAL WELFARE (RECIPROCITY AGREEMENTS, AND NEW ZEALAND ARTIFICIAL LIMB SERVICE) ACT 1990, SS.19C AND 19D AND SOCIAL WELFARE (RECIPROCITY WITH MALTA) ORDER 2013	
	COMPLIANCE
48. Malta/MSD Social Welfare Reciprocity To enable the transfer of applications for benefits and pensions, and advice of changes in circumstances, between New Zealand and Malta. Malta disclosure to MSD: Includes full name, date of birth, marital status, address, entitlement information and Maltese Identity Card and Social Security numbers. MSD disclosure to Malta: Includes full name, date of birth, marital status, address, entitlement information and New Zealand Client Number.	✓

SOCIAL WELFARE (RECIPROCITY AGREEMENTS, AND NEW ZEALAND ARTIFICIAL LIMB SERVICE) ACT 1990, SS.19C AND 19D AND SOCIAL WELFARE (RECIPROCITY WITH THE NETHERLANDS) ORDER 2003, ARTICLE 216	
	COMPLIANCE
49. 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.	✓
50. 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.	✓
51. 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.	✓

TAX ADMINISTRATION ACT 1994, S.82	
	COMPLIANCE
52. 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.	✓
53. 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.	✓
TAX ADMINISTRATION ACT 1994, S.83	
	COMPLIANCE
54. 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	
	COMPLIANCE
55. 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.	✓
TAX ADMINISTRATION ACT 1994, S.85	
	COMPLIANCE
56. 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.	✓

57. 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. Minor technical issue: The letter that IR sends individuals about suspension of WfFTC payments does not fully meet the notice requirements of section 103(1B) of the Privacy Act as it does not advise individuals that they have five working days to challenge the suspension. Individuals are advised they can contact IR if they think they qualify and IR states that business processes allow for an urgent refund to be paid within three days which reduces any risk of hardship to the customer if their entitlement is ceased incorrectly. We were satisfied with this approach. There have never been any reported cases identified.	X

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.

TABLE 1: RENEWED APPROVALS

USER AGENCY PROGRAMME NAME APPROVAL DATE	REASON	GROUNDS
ACC		
Prisoners 29 June 2015	Efficiency and security	Satisfactory audit result
DIA		
Passport eligibility (Citizenship) 22 December 2014	Efficiency and security	Satisfactory audit result
Passport eligibility (BDM) 22 December 2014	Efficiency and security	Satisfactory audit result
Citizenship application processing 22 December 2014	Efficiency and security	Timely delivery of data
DIA – IDENTITY VERIFICATION SERVICE		
Identity verification (Immigration) 2 June 2015	Efficiency and security	Satisfactory audit result
GOVERNMENT SUPER FUND		
Eligibility 18 May 2015	Efficiency and security	Satisfactory audit result
INLAND REVENUE		
Child support and student loans 1 July 2014	Efficiency and security	Temporary approval to remedy audit issues
Child support and student loans 1 September 2014	Efficiency and security	Temporary approval to remedy audit issues
Child support and student loans 29 September 2014	Efficiency and security	Audit issues remedied

Newborns tax number 19 December 2014	Efficiency and security	Security review planned
Newborns tax number 19 June 2015	Efficiency and security	Audit issues remedied or scheduled for completion
MINISTRY OF BUSINESS INNOVATION AND EMPLOYMENT		
Motor vehicle importers 22 June 2015	Efficiency and security	Audit issues remedied
Motor vehicle sellers 22 June 2015	Efficiency and security	Audit issues remedied
Prisoners (Immigration New Zealand) 29 June 2015	Efficiency and security	Satisfactory audit result
MINISTRY OF JUSTICE		
Fines defaulters tracing 9 January 2015	Efficiency and security	Satisfactory audit result
MINISTRY OF SOCIAL DEVELOPMENT		
Warrants to arrest 9 July 2014	Efficiency and security	Satisfactory audit result
Arrivals and departures 31 July 2014	Efficiency and security	Temporary approval to remedy audit issues
Arrivals and departures 29 September 2014	Efficiency and security	Timely delivery of data
General adjustment (Netherlands) 18 May 2015	Efficiency and security	Enhanced security measures
Deaths and marriages 9 June 2015	Efficiency and security	Enhanced security measures
Prisoners 29 June 2015	Efficiency and security	Satisfactory audit result
NATIONAL PROVIDENT FUND		
Eligibility 18 May 2015	Efficiency and security	Protections are automated