PRIVACY COMMISSIONER ANNUAL REPORT

2017

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 2017

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

November 2017

THE MINISTER OF JUSTICE

I tender my report as Privacy Commissioner for the year ended 30 June 2017

John Edwards
Privacy Commissioner

CONTENTS

FIGURES

APPENDICES

5 agencies

publicly named

for non-compliance with the Privacy Act

48%

of cases closed by settlement

TARGET: 40%

2,761

people completed online training modules

TARGET: 2,500

Provided advice on

186

proposals from agencies

TARGET: 100

Answered

7,320

enquiries from members of the public

TARGET: 7,500

Answered

8,433

questions through AskUs

Key points

Investigations and dispute resolution

- We continued to work hard to quickly and fairly resolve complaints. To this end, 90% of our cases were completed within 6 months, and nearly half of our closed cases were settled.
- Independent legal audits of our cases continue to indicate high quality processes. Each audit showed higher quality of process than the audit before, and the latest audit for this year gave a random selection of files an average mark of 4.25/5. We were very pleased with this result and the continuous improvement that led to it.
- We publicly named five agencies under our naming policy for non-compliance with the Privacy Act.

Litigation

- We referred four cases to the Director of Human Rights Proceedings.
- Thirty-seven complainants took cases to the Tribunal themselves.

Helping agencies share information

- We launched two new services to help agencies share information: advisory opinions and the Trusted Sharing Consultancy. Both of these services give agencies clarity about using the Privacy Act to share information.
- We were consulted by agencies on 186 proposals involving privacy issues.
- We published 22 submissions and other formal reports, including submissions to Select Committees.
- We reported to the Minister on two new Approved Information Sharing Agreements (AISAs).

Outreach and engagement

- During Privacy Week, we hosted five lunchtime seminars with other agencies and participated in five other agencies' internal privacy events to mark the week. These included public presentations by the Data Futures Partnership and the Broadcasting Standards Authority, and internal presentations at Air New Zealand and Auckland Council.
- We hosted a privacy research symposium in December 2016 to give researchers an opportunity to present their findings on a variety of social, health and educational privacy issues.
- We delivered 107 speeches and presentations and visited five regional centres.
- We responded to 7,320 public enquiries and 217 media enquiries.

Tools and resources to make privacy easy

- Early in the year we launched AskUs, our interactive FAQ, and it has received 8,433 questions from members of the public. We are constantly developing new content for AskUs, based on questions that users are asking.
- We launched three new online training modules: An Introduction to the Credit Reporting Privacy Code, Privacy and Employment, and Privacy ABC.

- During Privacy Week, we launched a wide variety of tools and resources such as guidance for taking health information offsite and a series of posters with useful privacy messages. We also published our first general privacy brochure, which gives an overview of privacy and everyday practical tips. This brochure is available in both English and Te Reo Māori.

Data breaches

- We received 132 voluntary data breach notifications from agencies.

International

- We approached the end of our three-year term of chairing and providing the secretariat of the International Conference of Data Protection and Privacy Commissioners. This was a successful term, where, among other things, we built a permanent conference website and document repository.
- We co-hosted (with the Australian Privacy Commissioner) a privacy enforcement workshop at the 47th Asia Pacific Privacy Authorities Forum (APPA). APPA has now grown to 20 authorities, with the privacy authorities from both Japan and the Philippines joining this year.

Codes of Practice

- We amended the Telecommunications Information Privacy Code to support a new system for sharing emergency caller location to enable emergency services to respond to 111 calls more quickly and accurately.
- We publicly notified proposals to amend the Health Information Privacy Code, the Telecommunications Information Privacy Code and the Credit Reporting Privacy Code in response to amendments made to the Privacy Act by the Intelligence and Security Act 2017.

Developments in privacy law

- The Supreme Court delivered a judgement clarifying the law in relation to voluntary requests for personal information by law enforcement agencies. The Supreme Court found that law enforcement agencies must provide sufficient detail to indicate the link between the offence being investigated and the requested information. This detail should give the agency responding to the request a reasonable belief that the disclosure is necessary.
- Through working with officials, Ministers and Select Committees, we secured improvements to a number of legislative proposals, including the Customs and Excise Bill, the Anti-Money Laundering and Countering Financing of Terrorism Amendment Bill and the Intelligence and Security Bill.
- We released an independent report into the Ministry of Social Development's proposal to require non-governmental organisations to collect, and pass on, individual-level data as a condition of funding from the Ministry.

Law reform

- We continued to work with officials to progress drafting of a new Privacy Act.

Introduction

During the reporting year, we have seen two key trends: increased demand from government and business to use personal information, and continued concern from the public to ensure this information is used appropriately, and kept safe.

In February 2017, the Data Futures Partnership published research from a series of workshops that investigated New Zealanders' attitudes towards government use of data. The research found (among other things) that people are more comfortable when they know why their data is being collected, who is going to use it and what it will be used for. Further, they were more comfortable if they knew they could see who had data about them and how it was being used.

These approaches, echoed in the structure of the Privacy Act itself, were particularly relevant this year, as more agencies pursued projects that involved large data sets.

Smart use of data has potential for positive impacts, but also carries risks. The positive impacts include more efficient resource allocation, while the risks include encoding biases and large-scale mistakes due to building systems based on flawed assumptions and inaccurate information.

We participated in a significant number of projects involving large data sets. Rather than choose between extracting value from the data and respecting personal privacy, we encouraged agencies to "have it both ways" by incorporating privacy values. Information privacy is built on accuracy and transparency. These values not only build customer trust, they also yield more robust data sets that are better-suited for guiding decision-making.

Carrots and sticks

Advising government agencies on new uses of personal information formed a significant proportion of our work this year. We launched two key services: advisory opinions and our Trusted Sharing Consultancy. Advisory opinions are a service where agencies can seek our view on how the law applies in a situation.

The Trusted Sharing Consultancy is a service to support agencies as they plan and implement initiatives that involve information sharing. There are many ways for agencies to achieve their policy objectives, such as consent-based sharing, Approved Information Sharing Agreements and codes of practice. The Consultancy Service helps agencies find the best fit for their initiative.

Part of our statutory role is to speak up when we think agencies are getting it wrong. We publicly named five agencies this year for non-compliance with the Privacy Act.

We also carried out an inquiry into a proposal by the Ministry of Social Development to collect individual client level data about people engaging with non-governmental organisations. Our inquiry found that the proposal carried a real risk of infringing on individual privacy. This inquiry resulted in the Ministry rethinking its plans to collect this level of data.

Influence through content

We've worked to extend our influence by creating content that allows more people to engage with our work.

One example is the launch of AskUs, our interactive online FAQs. AskUs answered more than 8,433 questions from the public. At the same time, there was only a slight decrease in the number of public enquiries via phone and email. This indicates that AskUs helped to significantly broaden our reach and educate the public about privacy issues.

We hosted a number of events to draw attention to privacy issues. One example was Privacy Research Week, where participants – including recipients of our Privacy Good Research Fund grants – presented their research into privacy issues. We also hosted multiple PrivacyLive forums, with guest speakers from a variety of different areas. This year, we made these events accessible to a wider audience by livestreaming them online. This ensured our events had far greater geographic reach.

Finally, we used our complaints function to provide content for blogs, case notes and media releases about cases with an important lesson or message. This approach allows us to extend the benefit of each case beyond the complainant and respondent of that case.

Guidance from the Supreme Court

The Privacy Act allows agencies to disclose information when it is necessary to avoid prejudice to the maintenance of the law. This issue came before the Supreme Court in a case in which we intervened in 2016, involving an electricity company. The Supreme Court delivered its judgment in March 2017, and confirmed that law enforcement agencies such as Police can ask government and private sector agencies for customer personal information under the Privacy Act without a mandatory demand such as a search warrant.

The Court found that both the requester and the agency holding the information have obligations to fulfil. The law enforcement agency must provide sufficient detail to indicate the link between the offence being investigated and the requested information. In complying with a request of this nature, the responding agency must be satisfied that disclosure is necessary to avoid prejudice to the maintenance of the law.

Responding to a law enforcement request is therefore a balance between responsible assistance to law enforcement and custodianship of the customer information. The privacy principles provide a guide for striking the right balance of when and what personal information should be released on a voluntary basis.

This decision gives us clear guidance for our decision-making. The Supreme Court's position echoes the position we have taken in cases involving the voluntary collection of personal information – such as our investigations into complaints by Nicky Hager and Martyn Bradbury (privacy.org.nz/hager and privacy.org.nz/bradbury). It was useful to see this approach supported by the Supreme Court.

Closing off as ICDPPC Chair

This year marks the completion of Privacy Commissioner John Edwards' three-year term as Chair of the International Conference of Data Protection and Privacy Commissioners (ICDPPC). We were proud to build the ICDPPC's online presence and accessibility by launching a website to host all of the Conference's content, as well as creating an ICDPPC Twitter account and a regular Conference newsletter. This has helped to keep stakeholders and regulators around the world informed about the Conference's activity and publications.

Report on activities

International

The connected nature of the global economy means that there is an underlying international dimension to many aspects of information privacy. This includes a significant amount of domestic activity. For example, a small business owner may use cloud-based email or document storage. Even if all of her customers are local, her – and their – information is now held overseas, and may be crossing borders as it goes from one server to the next.

For this reason, international relationships are important for providing protection to New Zealanders. Global privacy enforcement authorities need to cooperate across borders to protect against privacy threats from wherever they originate. Collaboration with counterpart authorities can lead to enhanced problem solving, creative policy solutions and more effective regulation. For example:

- International collaboration can lead to common standards to facilitate business transactions across borders in ways that protect the interests of individuals.
- A company's actions in one country can affect the citizens in another. For example, in the event of a security breach, we may need to seek the cooperation of 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 Forum (APPA)
- International Conference of Data Protection and Privacy Commissioners (ICDPPC)
- APEC Electronic Commerce Steering Group Data Privacy Subgroup (ECSG DPS)
- OECD Working Party on Security and Privacy in the Digital Economy (SPDE).

Highlights of 2016/2017

International Conference of Data Protection and Privacy Commissioners

Since 2014, the NZ Privacy Commissioner has served as elected Chair of the Conference, and has provided the Conference Secretariat. This responsibility ended in September 2017. The role of Chair and Secretariat has provided an opportunity to substantially contribute to advancing capacity building and strategic work amongst privacy and data protection authorities at an international level. Significant achievements have included, for example, building a permanent conference website and document repository, implementing an International Enforcement Cooperation Arrangement and running an international census of privacy regulators.

Asia Pacific Privacy Authorities Forum

We participated in the 45th and 46th forums in Singapore and Mexico and, just after the end of the reporting year, the 47th Forum in Sydney. The APPA Forum is continuing to build its importance in the region and has grown by two new members: the Japanese Personal Information Protection Commission and the National Privacy Commission of the Philippines. This brings the membership to 20 authorities, stretching from Colombia to Singapore. Alongside the 47th Forum, our office co-hosted a privacy enforcement workshop with the Australian Privacy Commissioner.

Global Privacy Enforcement Network (GPEN)

The GPEN network remains a key means of connecting with our international counterparts in enforcement. The Office regularly engages with GPEN, and participates in the annual GPEN Sweep.

APEC Electronic Commerce Steering Group Data Privacy Subgroup

A notable APEC achievement of the year was the adoption of a modernised APEC Privacy Framework. This was the direct result of a major project led by our office for the DPS in 2015.

OECD Working Party on Security and Privacy in the Digital Economy

Building upon the foundations laid last year at the OECD Ministerial Meeting in Cancun, Mexico, Assistant Commissioner Blair Stewart was invited by the OECD to present to SPDE expert meetings in Zurich and Paris to develop new privacy metrics for the digital economy. This work tied in with project work the office has been leading in APPA and ICDPPC.

Media, outreach and education

Our external communications aim to make privacy easy. This means helping individuals to be aware of their rights, and helping agencies to comply with the Privacy Act.

Some of our activity focuses on making material available online, in order to make it easier for people to quickly access privacy information. For example, we launched AskUs, an interactive FAQ with more than 400 common privacy questions. At the year's end, we received **8,433** enquiries through AskUs. At the same time, we received **7,320** public enquiries through our 0800 number and through email – slightly fewer than the **7,783** in the previous reporting year.

The slight drop in public enquiries, on top of the significant number of AskUs questions, indicate that AskUs has been a success. It suggests that there was significant unmet need for privacy advice. AskUs has significantly extended our influence by giving us the ability to answer over 100% more privacy questions than we could through our enquiries line.

AskUs is available at privacy.org.nz/ask.

Online training

Online training modules complement and extend our in-person training. This year, **3,807** people registered for at least one of our online training modules. This is significantly more people than we could train in person. We launched three new online training modules this year:

- An Introduction to the Credit Reporting Privacy Code (November 2016)
- Privacy in Employment (May 2017)
- Privacy ABC (June 2017)

Privacy in the employment relationship is a common thread across a diverse economy with all different varieties of agencies using personal information to achieve a variety of different goals. To this end, we launched Privacy in Employment in May 2017, in order to provide employers and employees with the information they need about their rights and responsibilities under the Privacy Act.

We developed An Introduction to the Credit Reporting Privacy Code under a similar theme. While people work and live in different circumstances, with different personal information requirements, credit reporting is a common thread that affects many people. For example, the credit reporting companies hold information about almost every utility customer's tendency to pay their bills, going back two years. With this in mind, we developed An Introduction to the Credit Reporting Privacy Code to help educate people about this common, and important, part of their lives.

We launched Privacy ABC to complement Privacy 101. Privacy 101 is an in-depth view of the Privacy Act that takes up to 3 hours to complete. Privacy ABC condenses the three hours of content in Privacy 101 into a 30-minute, scenario driven training module that gives a broad overview of people's rights and responsibilities under the Privacy Act.

FIG 1: ONLINE TRAINING MODULE REGISTRATIONS

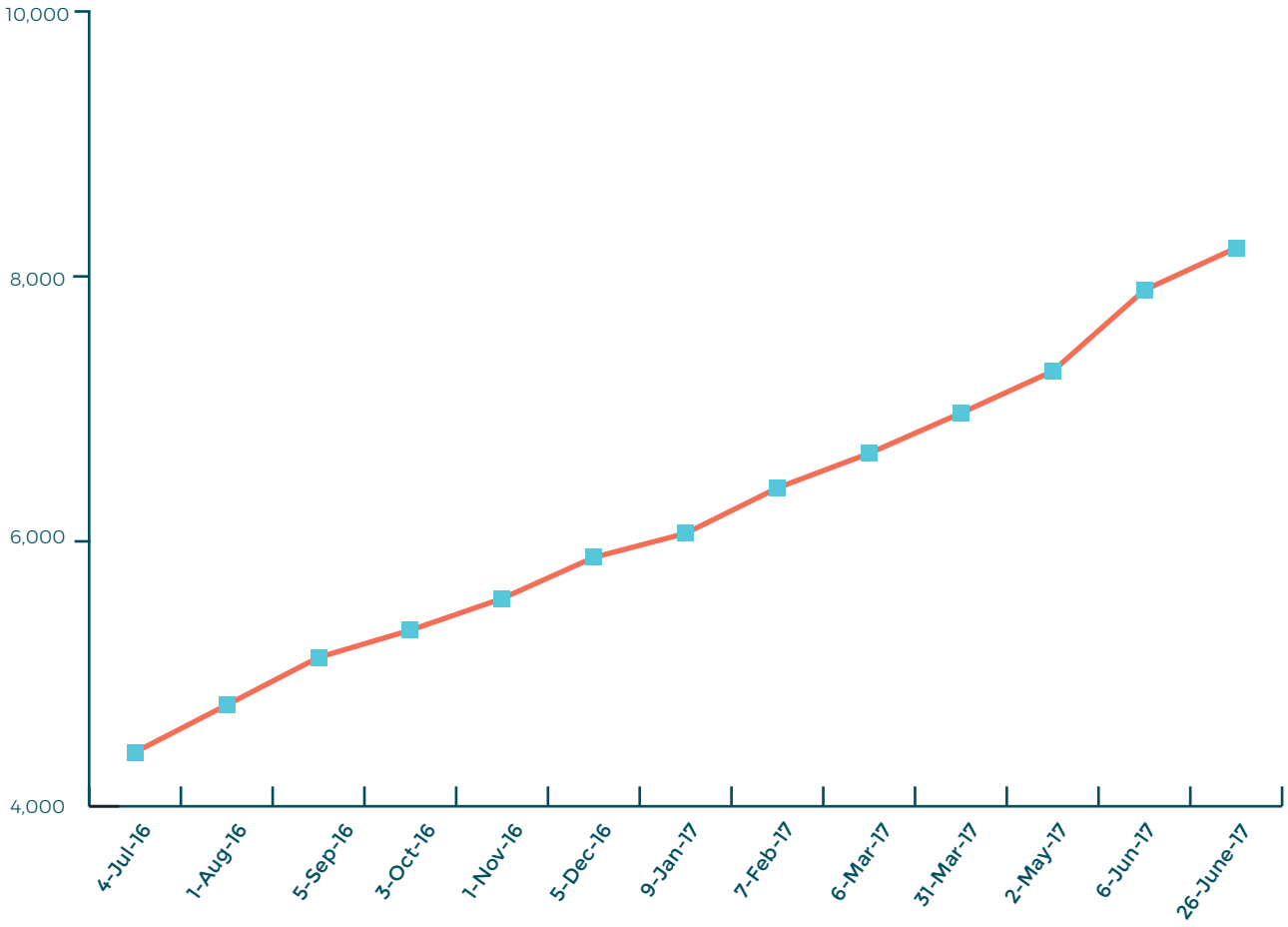
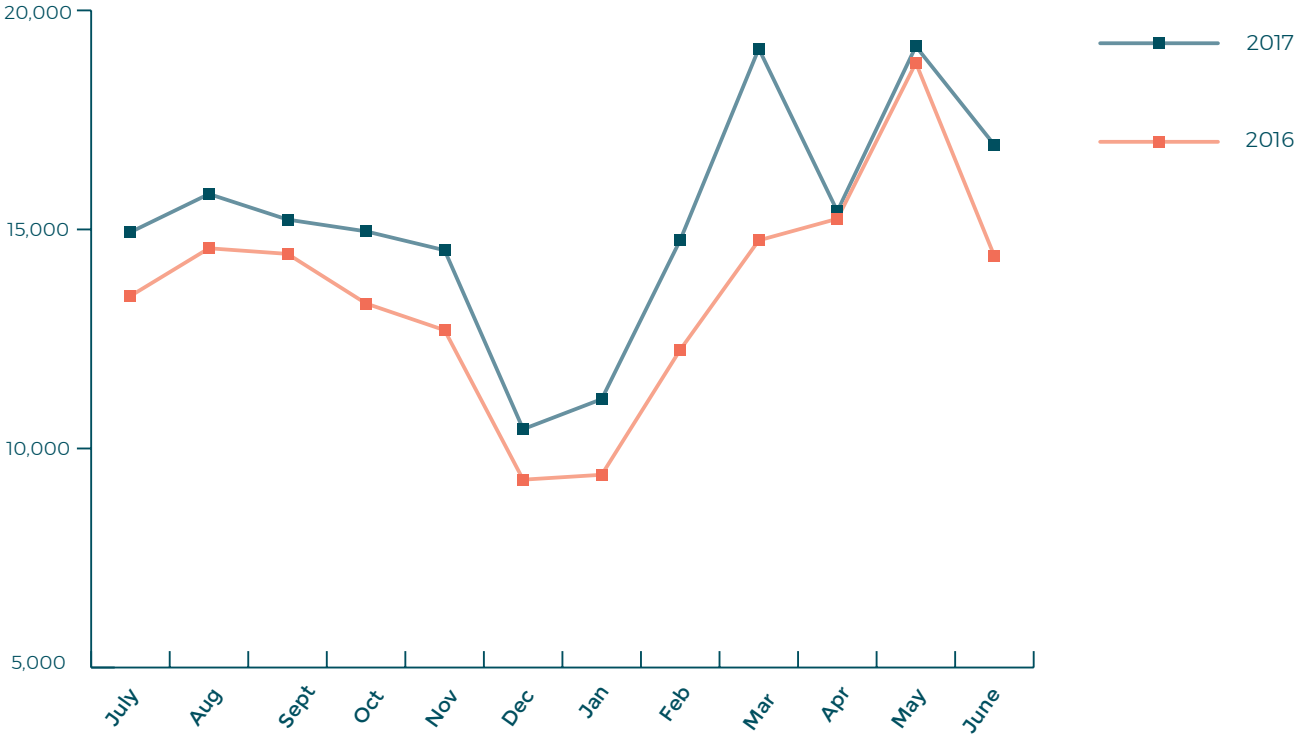


FIG 2: WEBSITE VISITORS



Where we would expect a privacy officer or privacy specialist to complete Privacy 101, Privacy ABC is pitched at a level suitable for raising privacy awareness right across an agency.

These modules have all seen strong growth, particularly Privacy ABC, which we launched in late June, and had more than 100 registrations when the financial year finished two weeks later. This growth has continued, with more than 500 registrations by the end of August 2017.

Value of a conversation

While online tools and engagement are useful to connect with people, there is still significant value in in-person engagement. For example, not everyone has a reliable internet connection. To this end, we continued to deliver speeches and presentations to a variety of audiences, with **107** delivered during the year.

We also continued our regional outreach strategy, meeting with civil society, business, and government stakeholders in five different regional centres. Upcoming visits are detailed on our website.

These outreach activities provide direct contact with individuals, communities and business groups. They are valuable points of engagement.

Privacy Week

Privacy Week is an opportunity for us to amplify privacy messages in one focussed week. This year's Privacy Week was 8-12 May, 2017.

This year saw significant amount of collaboration between our office and other agencies. We worked with the Data Futures Partnership, the Broadcasting Standards Authority and Internet New Zealand to put on a variety of lunchtime seminars. We also contributed to other agencies' events – for example, the Commissioner spoke at a privacy panel at Auckland City Council, and helped to launch Air New Zealand's updated privacy policy.

We streamed some of these seminars online, in order to increase our reach beyond the physical room. We received positive feedback about this approach from people all over the country.

We were pleased to see significant engagement on social media from other agencies in both the public and private sectors. This helped us to increase our influence by having other agencies distribute our message on our behalf.

As with most Privacy Weeks, we published new material – a general privacy brochure; guidance for health professionals when taking health information offsite; a new online training module on employment privacy, new case notes and a series of Privacy Week posters with helpful messages.

Privacy Good Research Symposium

In December 2016, we hosted a privacy research symposium to give researchers an opportunity to share understandings and present their findings on a variety of social, health and educational privacy issues. Some of this research was funded by grants from our Privacy Good Research Fund. The range of topics covered issues like note-taking by social workers and sexuality in aged care facilities.

The symposium demonstrated how privacy affects different parts of society and helped to develop the evidence base that underpins our public statements and advice. Hosting the symposium gave us the opportunity to lead these discussions about privacy, and use our networks and influence to further spread the outputs of those discussions.

Media

We received **217** media enquiries on a variety of topics. In previous years, our media enquiries have tended to "cluster" around a handful of large issues, but this year they were much more spread out, covering a range of issues. The exception to this was the April 2017 release of our report into the Ministry of Social Development's proposed collection of individual client level data, which generated a significant amount of media activity.

Investigations and dispute resolution

We continue to see positive results from our investigations and dispute resolution function:

- At year end, 90% of our files were less 6 months old – indicating that we are resolving issues quickly for complainants.
- Nearly half of the cases we closed were closed through settlement.

FIG 3: FILES CLOSED THROUGH SETTLEMENT

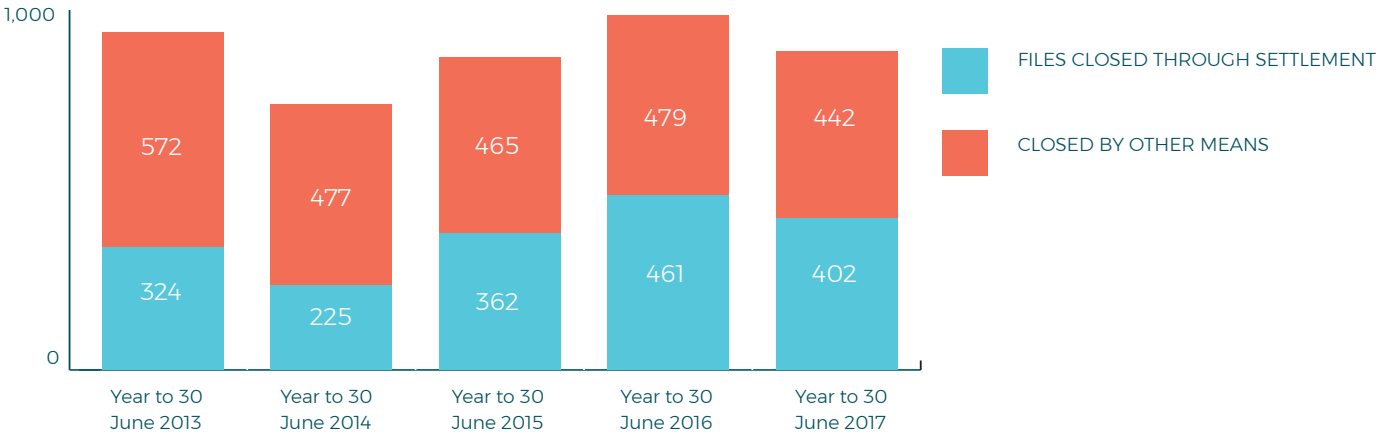
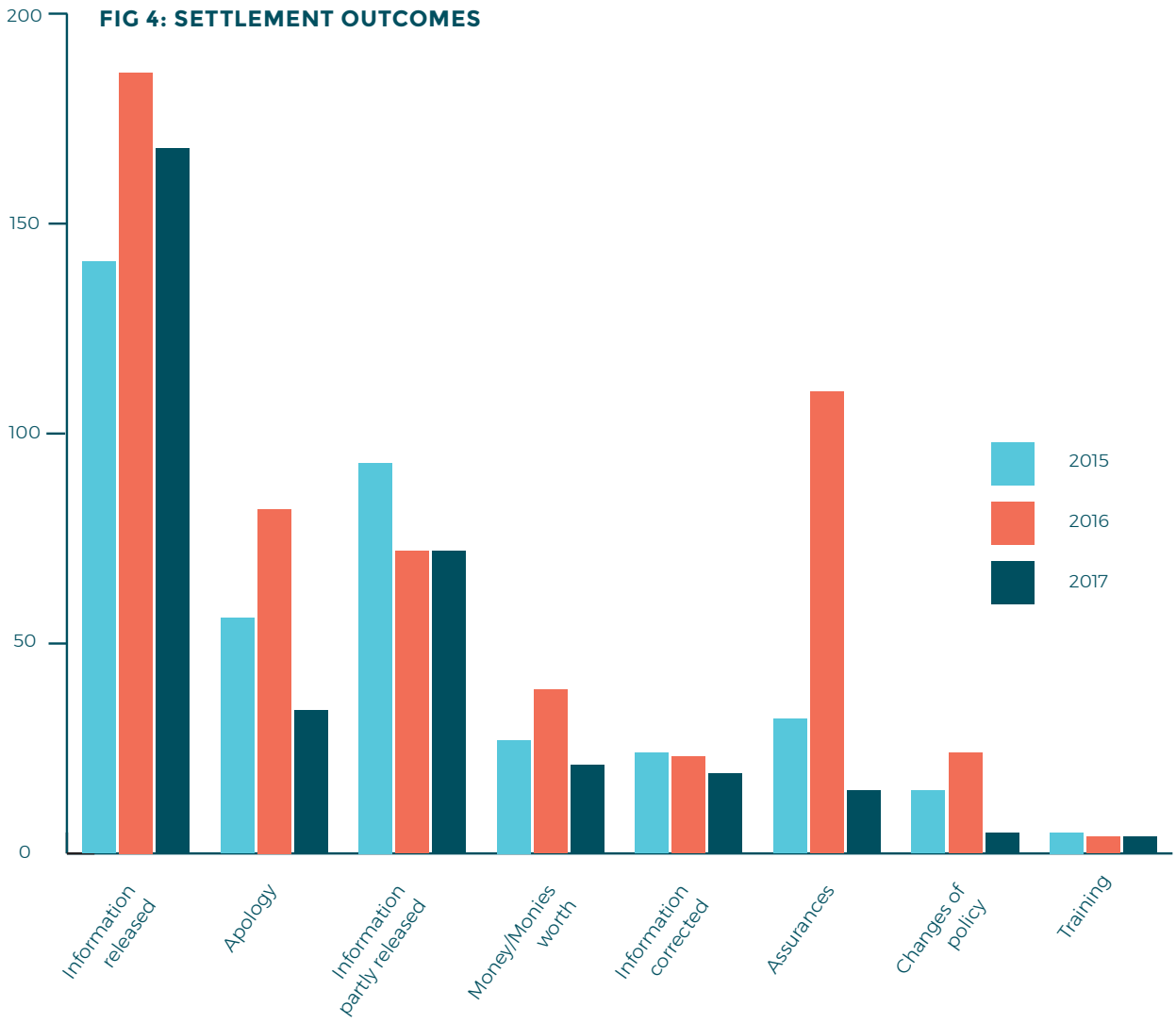


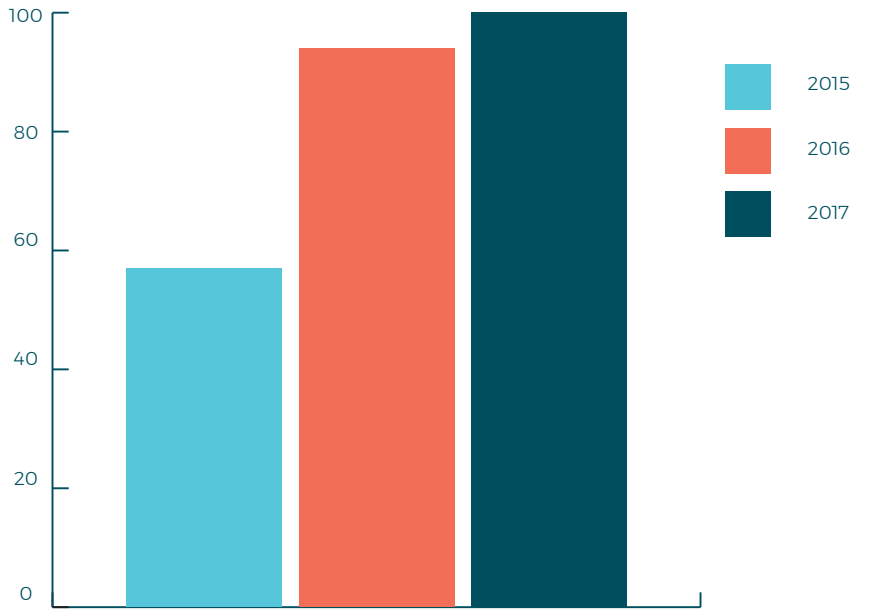
FIG 4: SETTLEMENT OUTCOMES



Quality of process

We continued to have regular external audits of our investigations. This is a process where a selection of investigations are reviewed and given a score out of 5 against a variety of criteria. Every audit has had a higher score than the previous audit, and the most recent score was an average of 4.25. This was a 100% achievement of our KPI in this area, which was for 85% of the externally reviewed complaints to be rated 3.5 or higher.

FIG 5: RESULT OF COMPLAINT FILE AUDITS

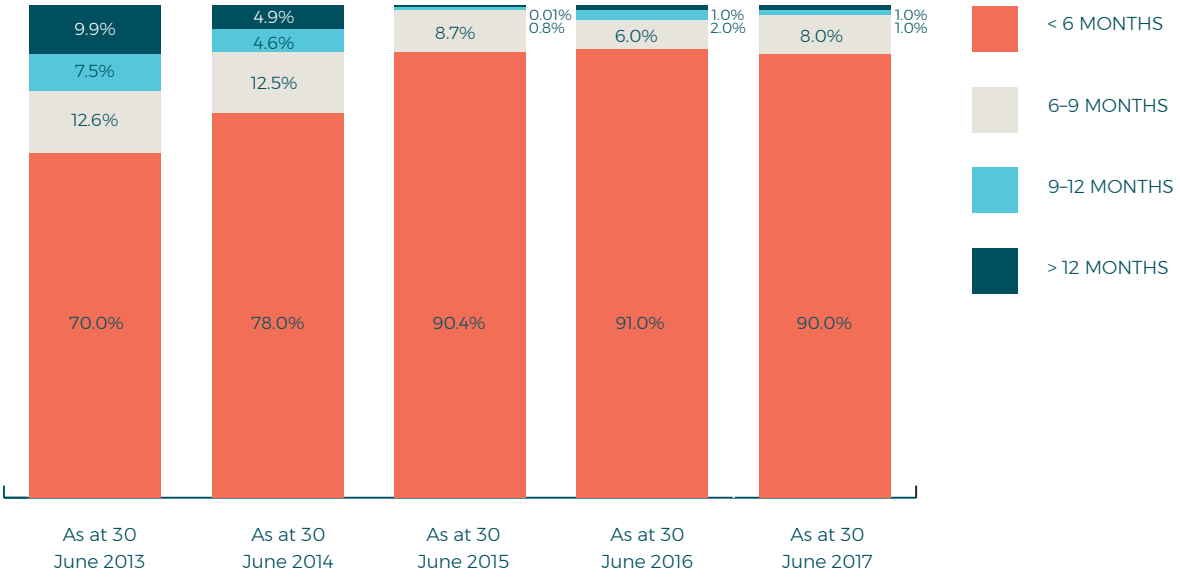


% rated 3.5 out of 5 or better for quality

Informing our communications

Our investigations team plays a wider role that goes beyond the resolution of each individual investigation. The team contributes content for many of our blogs, case notes, speeches, online training development and more. By maintaining a consistent feedback loop between our communications and investigations functions, we are able to ensure that our outreach material is both compelling and relevant by drawing on the stories that come from the investigations team. It also allows a "leverage" effect for investigators, as it gives the opportunity for certain cases to influence many more people than solely the individual complainant and the respondent agency.

FIG 6: COMPLAINTS WORK IN PROGRESS – AGE OF FILES



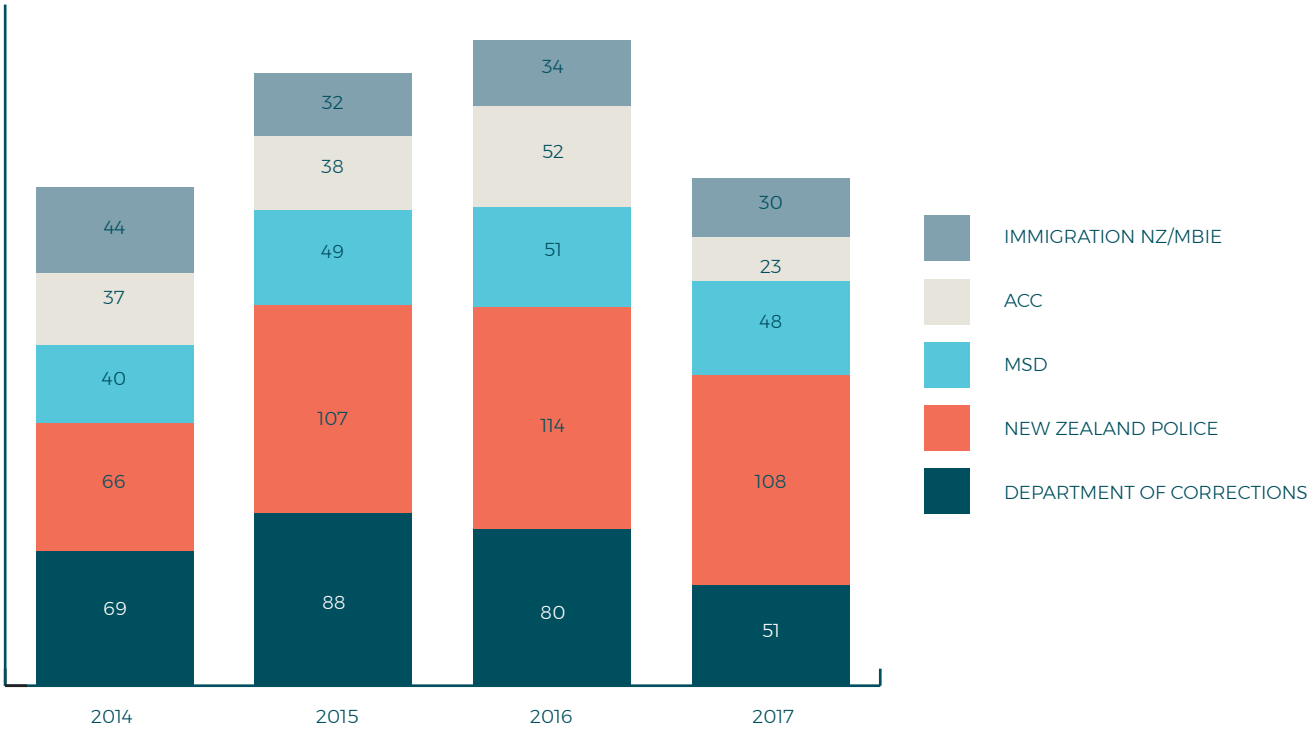
	COMPLAINTS RECEIVED 2016	COMPLAINTS RECEIVED 2017
Total complaints received	969	736
Received on-line	357	340
%	37%	46%

Building external capability

Our investigations team takes an active role in building capability in other agencies. For example, we trained three groups of editors for the newly-created Ministry for Vulnerable Children, Oranga Tamariki (MVCOT). These editors process Privacy Act and Official Information Act requests, so we were able to influence their practice by equipping them with relevant knowledge at a foundational level.

We also gave a variety of briefings and presentations to other agencies – such as guest lectures at Waikato University and a half-day workshop at the Asia Pacific Privacy Authorities (APPA) dispute resolution conference.

FIG 7: TOP COMPLAINTS BY AGENCY



	COMPLAINTS RECEIVED 2014	COMPLAINTS RECEIVED 2015	COMPLAINTS RECEIVED 2016	COMPLAINTS RECEIVED 2017
Department of Corrections	69	88	80	51
New Zealand Police	66	107	114	108
MSD	40	49	51	48
ACC	37	38	52	23
Immigration NZ/MBIE	44	32	34	30
Total	256	314	331	260
Total complaints received	725	836	969	736
% of total complaints received	**35.3%**	**37.6%**	**34.2%**	**35.3%**

CASE EXAMPLE

Disclosing information to protect children

A nanny was looking after children at an event run by the local council. A council officer saw how the nanny behaved with the children, and was concerned that she may be abusing them. The council officer called the agency that facilitated the nanny's employment and shared her concerns. The nanny complained to our office.

We found that there was no privacy breach, as agencies can disclose information if they think that doing so would prevent harm to someone's life or health. We also found that it did not matter whether the council officer was correct in her assumption – rather, the fact that she thought the children were in danger was enough to remove the agency's privacy liability.

Naming

Publicly naming organisations is one of the tools we use to promote compliance. We reserve this practice for specific situations, such as when an organisation does not engage with our investigation process, a privacy breach was particularly serious or if we suspect the agency's conduct may also affect other people.

This year we named five agencies:

- Expression Sessions – a photography company that breached principles 3, 4, 9 and 10 of the Privacy Act by taking pictures of a woman's children for her own use, then using those pictures for advertising.
- TD Drilling – a construction company that breached principles 5 and 6 of the Privacy Act by withholding and then losing employee information in an employment dispute.
- Law Debt – a debt collection agency that failed to check information about a disputed debt before referring the debt to a credit reporter.
- Department of Corrections – for refusing to release camera footage of a prisoner who was seriously assaulted.
- The Ministry of Social Development – for including inaccurate information about sexual offences in a man's file, in spite of multiple attempts by the man to correct the information.

CASE EXAMPLE

Police were right to disclose mental health information

A woman went into a police station to make a complaint about a hospital that had recently discharged her. The woman spoke to a constable and told him she had suicidal thoughts. The constable left the room and called an Emergency Mental Health Team.

The woman made a complaint to our office based on the constable passing on what she had told him. We found that there was no breach, as the constable had reasonable grounds to believe he was preventing or lessening a serious threat to her life by telling the Emergency Mental Health Team about her suicidal thoughts.

This is consistent with the Privacy Act – people can disclose information in order to protect other people from serious harm.

Litigation

Most complaints are resolved during the course of the investigation. 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 (HRRT). Complainants also have the right to take their case to the Tribunal themselves.

This year we referred four cases to the Director (an increase on the previous year) and proceedings have either been filed or will be filed in all four cases. These cases are in addition to those Director cases currently before the Tribunal from previous years, including one matter that was heard over two years ago and for which a decision has yet to be given.

Thirty-seven complainants took proceedings to the Tribunal themselves, without a referral from us (a slight increase on the previous year).

There continue to be substantial delays in the Tribunal both in delivery of decisions and in matters being heard. Unless the matter is urgent, it is likely to take two years before a hearing date is available. The Tribunal is faced with severe difficulties due to the increase in its workload, its resourcing, and legislative structure (that does not allow the appointment of a deputy chair to assist the Chairperson). The result is that it is unable to keep pace with the large inflow of new cases. The Chairperson has requested legislative amendments to allow the Tribunal – if adequately resourced – to hear and determine cases in a timely manner.

All but one of the Privacy Act cases decided by the Tribunal this year were dismissed, and there was no interference with privacy found. In the one case where an interference with privacy was found, a declaration was granted, but as damages were not claimed there was no award.

The High Court determined and granted one appeal from the Tribunal this year finding the Tribunal has wrongly struck out the plaintiff's claim for lack of jurisdiction as the Privacy Commissioner had conducted an investigation (*Edwards v CCDHB* HC decision [CIV 2016-475-487], 20 December 2016).

In March, the Supreme Court delivered a judgement in a case in which we intervened. The decision affirmed the importance and policy of the Privacy Act, and its relationship with other important statutes, including the production order regime in the Search and Surveillance Act 2012, the test for the admissibility of evidence under s 30 of the Evidence Act 2006 and the test for an unreasonable search under s 21 of the New Zealand Bill of Rights Act 1990. In particular, it clarified the law in relation to voluntary requests for personal information by law enforcement agencies, and affirms the obligations and responsibilities of both the law enforcement requester and the third party agency responding to a request. At the time of preparation of this report, the decision remains subject to to suppression orders.

Notable Tribunal decisions

Tan v New Zealand Police [2016] NZHRRT 32

This case involved a claim against the Police for collecting information from Tan's employer without her knowledge or a warrant, and in doing so disclosing sensitive personal information. The Police suspected Tan may have committed an offence by inappropriately accessing the National Health Index (NHI) database through her role at the DHB to try and locate family members who had a secret address for their own safety, as they were the victims of crimes committed by her brother. The Police disclosed background information to the DHB that included her brother's convictions for child sexual and physical abuse and possessing child pornography. The DHB's internal investigation showed she had not accessed the NHI or DHB databases.

The Tribunal dismissed the claim, finding no interference with privacy as there was no breach of either the collection principles (principles 1-4) or the disclosure principle (principle 11). The Tribunal found that the privacy principles were flexible enough for this kind of request to be made by law enforcement agencies, as there was insufficient evidence to obtain a compulsory order. Police were able to satisfy the criteria to enable them to rely on the maintenance of the law exceptions.

The Tribunal does not always award costs to successful defending agencies, so as not to deter people from bringing a case, but it did so here. The Tribunal awarded Police costs of $1,500, recognising that the plaintiff's conduct had needlessly added to the difficulty and cost of proceedings. Police had sought $4,000 as a contribution to their costs of $28,800.

Yiasoumi v Attorney General [2017] NZHRRT 12

The Tribunal found there had been no interference with Mr Yiasoumi's privacy and that an agency is not required to apply unlimited resources to locate requested information, even when the information is really important to the requester. While the Police did carry out an exhaustive inquiry into the photographs, a 'no stone unturned' inquiry is not the standard set by the Privacy Act.

The Tribunal found that Police were justified in refusing Mr Yiasoumi's request on the grounds the information did not exist, or could not at the time be found. (Due to human error, the record of the photos sought were not placed in the file management centre, but remained in the officer's personal folder. Once the photos were eventually found, they were sent to Mr Yiasoumi.)

The case illustrates that organisations sometimes get it wrong when they respond to a person's request for their personal information; information is sometimes lost, displaced or accidentally deleted. It also demonstrates the importance of a requester being specific and giving the surrounding context for their request.

Codes of practice

At the start of the year there were six codes of practice in force. During the year we amended the Telecommunications Information Privacy Code, and towards the end of the year we sought public submissions on proposals to amend three codes.

Telecommunications Information Privacy Code

We amended the Telecommunications Information Privacy Code in January, following a public submission process. The amendment supported a new system for sharing emergency caller location information to enable the emergency services to respond to 111 calls more quickly and accurately. This amendment came into force in March.

Each year more than one million calls are transferred to the emergency services. In the year preceding the establishment of the new system, the NZ Police had recorded 1,800 incidents in which caller location information needed to be requested from a network operator under the old manual system. The new system automatically generates information on mobile caller location and enables its release. The amendment enables the system to be operated lawfully, even though the caller is not asked to consent to the location tracking. The amendment imposes certain safeguards and controls.

Amending three codes

In June, we publicly notified proposals to amend the Health Information Privacy Code, Telecommunications Information Privacy Code and the Credit Reporting Privacy Code. The closing date for submissions fell after the end of the reporting year. The proposed amendments were in response to amendments made to the Privacy Act by the Intelligence and Security Act 2017. The amendments to the codes will come into effect later in 2017 to coincide with commencement of the amendments to the Privacy Act and to maintain a degree of consistency between Act and codes, except where differences are warranted.

Security and Intelligence Amendment Bill

This Bill made changes to key aspects of New Zealand's security and intelligence services. It was the output of the independent review of the Security and Intelligence Act from 2015.

In the 2015 review, we recommended that the GCSB and NZSIS should be subject to all of the principles in the Privacy Act. These recommendations were largely taken on board in this year's amendment Bill.

These agencies are now subject to every principle, except for principles 2, 3 and 4(b).

We also supported the inclusion of a new exception to principles 10 and 11, which respectively refer to the use and disclosure of personal information. This exception applies to intelligence agencies when using or disclosing information is necessary to enable the performance of any of their functions. This is an improvement on the previous situation where NZSIS and GCSB were exempted from most of the privacy principles.

We are pleased to be able to tell our international counterparts that New Zealand's security and intelligence agencies are subject to some of the most robust oversight and transparency in the world.

Policy

Our policy work involves the entire policy life cycle – from policy development with agencies and ministries, to providing input to Cabinet papers, to submitting formally on legislation.

We have advised on 186 proposals from agencies that involved personal information, and published 22 submissions and formal reports.

Privacy impact assessments

We provided advice on a significant number of privacy impact assessments (PIAs). These are a systematic process for assessing privacy risks and potential mitigations for those risks when implementing a new initiative that may have an effect on personal information.

The privacy impact assessments we reviewed this year showed a major shift in approach. In the past, PIAs tended to focus on reputational risks to the organisation. Now, PIAs are giving greater weight to direct impacts on individual privacy. This customer-first approach drives better outcomes for individuals while also helping the agency mitigate reputational risks.

Social investment

We gave advice on the developing social investment approach. By its very nature, social investment requires a significant amount of personal information, as it uses large data sets to help develop evidence about how best to allocate social spending.

We helped agencies consider how to safely collect the information they needed while also helping them to maintain the trust and confidence of New Zealanders through good information handling practices. This included advocating for strong security and accuracy policies, making sure people know what information is being collected and why, and ensuring people are able to exercise control over their personal information.

These approaches gave agencies the information they needed while also enhancing trust in the overall system.

Anti-Money Laundering and Countering Financing of Terrorism Amendment Bill

The Anti-Money Laundering and Countering Financing of Terrorism Act 2009 placed obligations on agencies that handled information in order to detect and deter money laundering and terrorist financing. In 2017, the Anti-Money Laundering and Countering Financing of Terrorism Amendment Bill extended the 2009 Act.

We worked with officials and Parliament to highlight areas of concern in the information sharing components of the Bill. For example, we advised that the information powers be limited to information that was not personal information. Parliament adopted this advice.

The Bill also gave agencies authority to enter into agreements giving broad access to individuals' data. The Select Committee agreed with our recommendation that this clause of the Bill be removed.

Police vetting

Police vetting is a process by which certain agencies – such as schools and hospitals – can have people (such as potential employees and volunteers) vetted by Police. This is more extensive than a background check for criminal convictions, and may include a range of other interactions between an individual and Police.

Every year, more than 500,000 people undergo police vetting. This number is likely to grow as the Vulnerable Children's Act makes police vetting a requirement.

Police asked our office and the Independent Police Conduct Authority to investigate this process and make recommendations. We found that while most police vets were straightforward, there was a minority (roughly two percent) where Police had to make a decision about whether to disclose information other than convictions to

the requesting authority. While this was a small proportion, it still represented up to 10,000 people per year, so it is significant.

We recommended a clearer framework for decision-making about these "line calls." This increased transparency for the subjects of police vetting.

Trusted sharing consultancy

In keeping with our overall goal to help agencies use the Privacy Act as enabling legislation, we launched the Trusted Sharing Consultancy Service in late 2016. This is a new service to help agencies use the Privacy Act to enable information sharing. We worked with agencies at an early stage of information sharing projects, finding ways to achieve their goals using the existing parameters of the Privacy Act.

We did not approach this in a rigid way. Rather than only focusing on ways to use the Privacy Act to achieve information sharing goals, we worked with agencies to achieve their wider goals, which could sometimes be accomplished without sharing information. This helped agencies get their jobs done in easier, less time-consuming ways, and without compromising individual privacy.

The Trusted Sharing Consultancy helped with a number of proposals, such as supporting the Department of Internal Affairs in its efforts to increase self-service tools, and supporting Police, DIA, NZTA and Immigration NewZealand to develop mechanisms for sharing information to enhance identity verification at New Zealand's borders.

Helping local government use cameras

A local council approached us requesting our feedback on a proposal to equip parking wardens with body cameras. Among other things, the local council sought our authorisation to collect personal information in a way that it thought would be a breach of a privacy principle. We advised the local council that its policy did not seek to breach a privacy principle, so it did not require our authorisation. This clarity around the structure of the Privacy Act was useful for the local council, as it gave the council the certainty it needed to implement its cameras.

Advisory opinions

Advisory opinions are another tool we launched to give agencies greater certainty about our approach to the law. This is where agencies can seek our view on an issue. This provides certainty about the privacy impact of a proposed process, service or other use of personal information. Under this policy, agencies can seek our view on how we would interpret the law in relation to a proposal or scenario.

We published one advisory opinion this year, for the NZ Fire Service. It is available on our website.

Inquiry into individual client level data

We conducted an inquiry into the Ministry of Social Development's collection of individual client level data (ICLD). This proposed initiative by the Ministry of Social Development required non-governmental organisations to provide specific client data – such as name, address and date of birth – as a condition of receiving funding from the Ministry. This included NGOs that deal with sensitive issues such as psychological counselling and family violence.

We undertook an inquiry into the proposed policy and contract changes, and found that while the objectives were well-intentioned, the Ministry had not given adequate consideration to whether it could meet those objectives without collecting such a granular level of personal information. We released a report on our inquiry in April 2017, and in May the Ministry announced that it would no longer be requiring non-governmental organisations to pass on individual client level data.

Approved Information Sharing Agreements (AISAs)

AISAs are mechanisms that allow agencies to collaborate and share information without intruding on individual privacy.

Two agencies completed AISAs during the reporting year:

- An AISA allowing the Ministry of Justice to share court information with Statistics New Zealand, in order to inform the Integrated Data Infrastructure, which in turn helps inform solutions to solve social issues in New Zealand.
- An AISA allowing the Ministry of Education to share information with MSD's Youth Services to identify and encourage young people who have ceased to be enrolled at school or a tertiary education organisation to move into or remain in, education, training, and employment.

Reviewing the Privacy Act

In 2014, the Minister of Justice announced the Government's intention to reform the Privacy Act to align it with technological change. This was based on recommendations from the Law Commission in 2011. The Government has not yet introduced legislation to reform the Privacy Act to Parliament.

We have a statutory responsibility to periodically review the Privacy Act, consider whether it needs to be amended and to report our views to the Minister of Justice. This year, we reviewed the Act to identify any further reforms that would strengthen the Act, in addition to the reforms proposed in 2014.

In February 2017, the Minister formally tabled our report in Parliament. This report called for:

- A right to data portability
- Controls on re-identification – which is identifying people in anonymous data sets by cross-referencing two different, anonymised data sets
- A new power to require agencies to demonstrate compliance with the Act
- A new civil penalty for serious or repeated breaches of the Act
- Narrowing defences available to those who obstruct our investigations, or fail to comply with a lawful requirement from our office
- Reforming the public register principles in the Act and providing for the suppression of personal information in public registers where there is a safety risk.

While the Privacy Act's principles-based approach is largely still fit for purpose, there are areas where adjustments need to be made to match the Act with the technological landscape. The above recommendations would bring the Act in line with current technology, as well as improve our ability to enforce the law.

Family and Whānau Violence Legislation Bill

We worked with officials to help define the information sharing components of this Bill, and then made a formal submission to the Justice and Electoral Committee.

We recommended that clause 124V(5) be removed from the Bill. The clause called for agencies and practitioners to prioritise safety over confidentiality. We recommended this clause to be removed, as the two concepts are not mutually exclusive. In addition, section 7 of the Privacy Act already means that the enabling information sharing provision in the Bill takes precedence. The clause was later amended to specify that it authorised, but did not require practitioners to share information.

We also drew the Committee's attention to the inconsistency in the approach being advanced in the information sharing regime in this Bill and that in the Children, Young Persons and their Families (Oranga Tamariki) Legislation Bill. We advised that the two pieces of legislation should be aligned, as there was a risk they would create significance confusion and difficulty in the great number of cases that involve both family violence and child abuse. Our view was that the approach in the Family and Whānau Violence Legislation Bill was to be preferred.

We advised that guidance around when to share information would be better placed in code of practice, and that there should be a requirement to consult the Privacy Commissioner before such codes are finalised.

Enhancing Identity Verification and Border Processes Legislation Bill

This was an omnibus bill that increased information sharing between agencies, after the inquiry into the escape of Philip John Smith / Traynor.

Our initial feedback on this process was that the Privacy Act already had sufficient information sharing mechanisms.

On the Bill itself, we suggested a number of additional safeguards on the information sharing. For example, we suggested that Police access to Customs information should be on a case-by-case basis, as Customs have much more intrusive powers to collect information at the border than other agencies do in other situations.

Our recommendations were not implemented.

Customs and Excise Bill

Customs consulted us through the policy development behind this Bill, particularly in respect to searching electronic devices. We advised that powers to search electronic devices at the border should be proportionate, because devices hold significant amounts of personal, sensitive information. Unfettered powers to search electronic devices would be a significant intrusion into both the phone's owner's information, and also into the information of those he or she interacts with.

We recommended that Customs officers should have to reach a level of suspicion before they can access an electronic device.

The current draft of the Bill reflects this advice, drawing a distinction between an "initial search" and a "full search." Under this drafting, a Customs officer would have to have reason to believe there is evidential material on the device before undertaking a full search, which would involve unlocking the device.

Auditing policy processes

We routinely employ third-party auditors to examine a random sample of policy files. This year, the independent auditor gave the following feedback:

> **"OPC substantially achieved its performance expectations for the quality of policy and the quality of information sharing / matching outputs, as noted in the Privacy Commissioner's Statement of Performance Expectations 2016-17. 80% of the files assessed met or exceeded OPCs quality standards (ie rated 3½ or better), based on the findings from my independent review of a sample of policy files closed in the year. This result was consistent for both the policy files and the information sharing / matching files.**
>
> **It is clear that overall OPC provides high quality advice, that is typically exemplary of good practice.**
>
> **The assessment was undertaken in a way consistent with the assessment of technical quality of policy advice that government departments with policy appropriations are required to report against. Care needs to be taken with comparing this result with previous years, as the methodology is different to that used in prior years."**

POLICY – SATISFACTION WITH ADVICE (FROM ANNUAL STAKEHOLDER SURVEY)

	2015	2016	2017
% of respondents rating they are satisfied with the service provided	91%	90%	93%

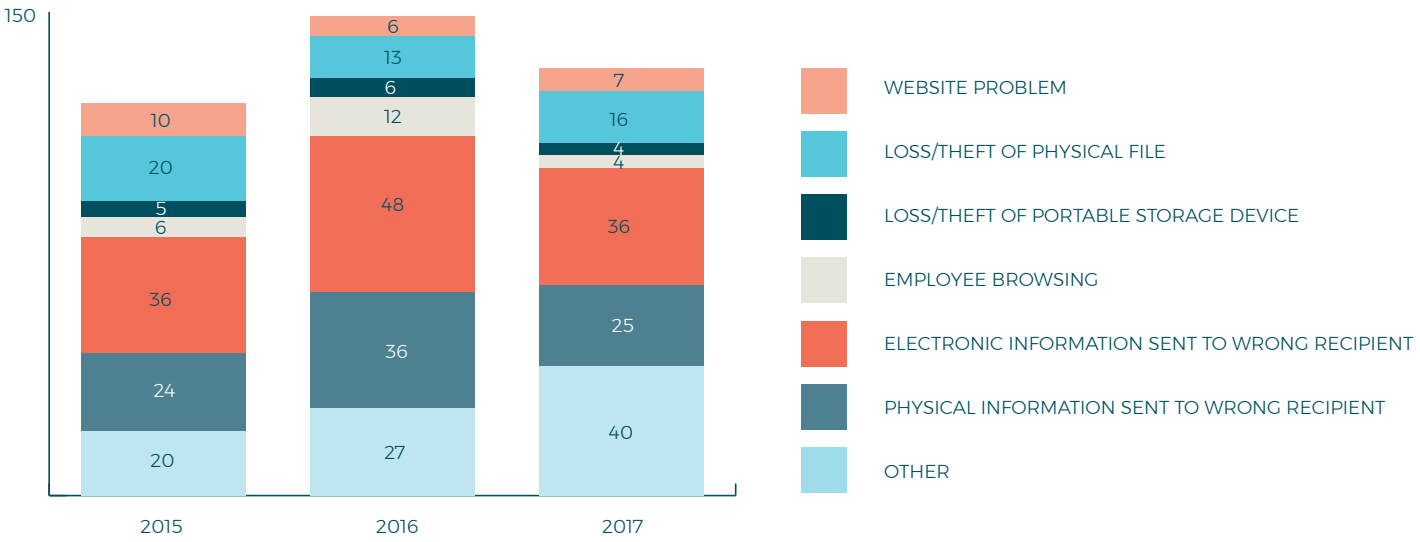
Breach notifications

We receive breach notifications from a variety of public and private sector agencies. Breach reporting remains voluntary, so there is no way of knowing what proportion of all breaches that occur are reported to our office.

This year 132 breaches were reported.

Common types of breaches

FIG 8: COMMON TYPES OF BREACHES



The most common cause of a privacy breach is human error or carelessness, however, this is often influenced by the way processes and systems are designed.

To strengthen our contribution in this area we have dedicated part of a role to breach notifications. This has resulted in:

- The ability to provide more supportive engagement when agencies notify breaches.
- Improvements to the quality of the information we record.
- An ongoing series of blog posts based on actual breaches to highlight how breaches occur and steps that can be taken to reduce their likelihood or their impact.

We are working to improve reporting of breaches by:

- Demonstrating to agencies the value of their reports through the lessons shared.
- Looking at international developments in categorising the types of breaches.
- Liaising with CERT NZ to share information about breaches.

Breach case: unclear document name leads to breach

Files sent to the wrong person are a common source of privacy breaches. In one case, this happened because a file that was sent by accident had a very similar name to the file that should have been sent.

The lesson from this breach was that underlying processes and procedures – such as naming conventions – need to be built to reduce the likelihood of human error.

Information Matching

Statutory review of information matching provisions

The Privacy Act requires the Privacy Commissioner to review the operation of each information matching provision every five years. In these reviews, the Commissioner recommends whether a provision should continue, be amended or be cancelled.

This year the Privacy Commissioner reviewed two information matching provisions and considered that they should be continued without amendment:

Electoral Act 1993, section 263B

This allows the Electoral Commission access to information on people who may be qualified to be on the electoral roll but who have not yet registered, or who are on the roll but whose details have changed. Information comes from the data sets of beneficiaries, students, driver licences, vehicle registrations, new citizens and passports.

Immigration Act 2009, section 300

This allows the Ministry of Health to access information from Immigration New Zealand to determine an individual's eligibility for access to publically funded health and disability support services.

The review reports are available on our website: **https://privacy.org.nz/privacy-for-agencies/information-sharing/information-matching-reports-and-reviews/**

Changes in authorised and operating programmes

Currently operating:

There are currently 52 information matching programmes in operation (see Appendix B which also includes the 1 programme that ceased in the year).

New provisions and programmes:

Parliament passed no new information matching provisions during the year.

Inland Revenue (IR) started operating a programme with death information from the Department of Internal Affairs.

Programmes suspended:

The Ministry of Business, Innovation and Employment did not operate their programme with the New Zealand Customs Service to identify people who might qualify as motor vehicle traders.

The Ministry of Justice ceased to operate their programme with Immigration New Zealand because of the significant manual effort involved and the comparatively low benefits from the programme.

The Ministry of Social Development (MSD) did not operate their Periods of Residence sampling match with Australia for superannuation entitlement. MSD advise that Australia's concerns with Australian privacy law have been resolved and therefore they may resume operating the programme.

MSD also did not need to use the provision to allow IR to respond to tax information enquires from the Netherlands social welfare authorities, as no requests were received from the Netherlands.

Programmes ceasing:

Five of the current information matches between IR and MSD were replaced by an Approved Information Sharing Agreement on 31 August 2017.

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 investigations teams across offices, 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 all corporate support functions including administrative, financial, information technology, performance measurement 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 and Privacy Act law reform.

EEO profile

We promote Equal Employment Opportunities (EEO) to ensure that our people capability practices are in line with our 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 policies on recruitment, employee development, harassment prevention and health and safety.

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

- Developing talent 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.

AS AT 30 JUNE 2017

	WOMEN		MEN		TOTAL
	FULL-TIME	PART-TIME	FULL-TIME	PART-TIME	
Commissioner			1		1
Senior managers	3		2		5
Team leaders/Senior advisers	4	1			5
Investigating officers	4	1	2		7
Administrative support	7	1			8
Advisers (technology, policy, communications, codes and general counsel)	4		5		9
Enquiries officers	1	1			2
Total	23	4	10		37

	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									5	
Team leaders/Senior advisers	1				1				2	1
Investigating officers	1								5	1
Administrative support									7	1
Advisers (technology, policy, communications, codes and general counsel)					1		1		7	
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 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.

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 2017

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 his behalf.

Opinion

We have audited:

- the financial statements of the Privacy Commissioner on pages 45 to 60, that comprise the statement of financial position as at 30 June 2017, the statement of comprehensive revenue and expenses, statement of changes in equity and statement of cash flows for the year ended on that date and the notes to the financial statements including a summary of significant accounting policies and other explanatory information; and
- the performance information of the Privacy Commissioner on pages 37 to 45.

In our opinion:

- the financial statements of the of the Privacy Commissioner on pages 45 to 60:
    - present fairly, in all material respects:
        - its financial position as at 30 June 2017; and
        - 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 Regime.
- the performance information on pages 37 to 45:
    - presents fairly, in all material respects, the Privacy Commissioner's performance for the year ended 30 June 2017, including:
        - for each class of reportable outputs:
            - its standards of delivery 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; and
- what has been achieved with the appropriation; and

- 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 25 October 2017. This is the date at which our opinion is expressed.

The basis for our opinion is explained below. In addition, we outline the responsibilities of the Privacy Commissioner and our responsibilities relating to the financial statements and the performance information, we comment on other information, and we explain our independence.

Basis for our opinion

We carried out our audit in accordance with the Auditor-General's Auditing Standards, which incorporate the Professional and Ethical Standards and the International Standards on Auditing (New Zealand) issued by the New Zealand Auditing and Assurance Standards Board. Our responsibilities under those standards are further described in the Responsibilities of the auditor section of our report.

We have fulfilled our responsibilities in accordance with the Auditor-General's Auditing Standards.

We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our audit opinion.

Responsibilities of the Privacy Commissioner for the financial statements and the performance information

The Privacy Commissioner is responsible for preparing financial statements and performance information that are fairly presented and comply with generally accepted accounting practice in New Zealand. The Privacy Commissioner is responsible for such internal control as it determines is necessary to enable it to prepare financial statements and performance information that are free from material misstatement, whether due to fraud or error.

In preparing the financial statements and the performance information, the Privacy Commissioner is responsible for assessing the Privacy Commissioner's ability to continue as a going concern. The Privacy Commissioner is also responsible for disclosing, as applicable, matters related to going concern and using the going concern basis of accounting, unless there is an intention to merge or to terminate the activities of the Privacy Commissioner or there is no realistic alternative but to do so.

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

Responsibilities of the auditor for the audit of the financial statements and the performance information

Our objectives are to obtain reasonable assurance about whether the financial statements and the performance information, as a whole, are free from material misstatement, whether due to fraud or error, and to issue an auditor's report that includes our opinion.

Reasonable assurance is a high level of assurance, but is not a guarantee that an audit carried out in accordance with the Auditor-General's Auditing Standards will always detect a material misstatement when it exists. Misstatements are differences or omissions of amounts or disclosures, and can arise from fraud or error. Misstatements are considered material if, individually or in the aggregate, they could reasonably be expected to influence the decisions of readers, taken on the basis of these financial statements and the performance information.

For the budget information reported in the financial statements and the performance information, our procedures were limited to checking that the information agreed to the Privacy Commissioner's statement of performance expectations.

We did not evaluate the security and controls over the electronic publication of the financial statements and the performance information.

As part of an audit in accordance with the Auditor-General's Auditing Standards, we exercise professional judgement and maintain professional scepticism throughout the audit. Also:

- We identify and assess the risks of material misstatement of the financial statements and the performance information, whether due to fraud or error, design and perform audit procedures responsive to those risks, and obtain audit evidence that is sufficient and appropriate to provide a basis for our opinion. The risk of not detecting a material misstatement resulting from fraud is higher than for one resulting from error, as fraud may involve collusion, forgery, intentional omissions, misrepresentations, or the override of internal control.

- We obtain an understanding of internal control relevant to the audit 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.

- We evaluate the appropriateness of accounting policies used and the reasonableness of accounting estimates and related disclosures made by the Privacy Commissioner.

- We evaluate the appropriateness of the reported performance information within the Privacy Commissioner's framework for reporting its performance.

- We conclude on the appropriateness of the use of the going concern basis of accounting by the Privacy Commissioner and, based on the audit evidence obtained, whether a material uncertainty exists related to events or conditions that may cast significant doubt on the Privacy Commissioner's ability to continue as a going concern. If we conclude that a material uncertainty exists, we are required to draw attention in our auditor's report to the related disclosures in the financial statements and the performance information or, if such disclosures are inadequate, to modify our opinion. Our conclusions are based on the audit evidence obtained up to the date of our auditor's report. However, future events or conditions may cause the Privacy Commissioner to cease to continue as a going concern.

- We evaluate the overall presentation, structure and content of the financial statements and the performance information, including the disclosures, and whether the financial statements and the performance information represent the underlying transactions and events in a manner that achieves fair presentation.

We communicate with the Privacy Commissioner regarding, among other matters, the planned scope and timing of the audit and significant audit findings, including any significant deficiencies in internal control that we identify during our audit.

Our responsibilities arise from the Public Audit Act 2001.

Other information

The Privacy Commissioner is responsible for the other information. The other information comprises the information included on pages 8 to 31, 36 and 61 to 73, but does not include the financial statements and the performance information, and our auditor's report thereon.

Our opinion on the financial statements and the performance information does not cover the other information and we do not express any form of audit opinion or assurance conclusion thereon.

In connection with our audit of the financial statements and the performance information, our responsibility is to read the other information. In doing so, we consider whether the other information is materially inconsistent with the financial statements and the performance information or our knowledge obtained in the audit, or otherwise appears to be materially misstated. If, based on our work, we conclude that there is a material misstatement of this other information, we are required to report that fact. We have nothing to report in this regard.

Independence

We are independent of the Privacy Commissioner in accordance with the independence requirements of the Auditor-General's Auditing Standards, which incorporate the independence requirements of Professional and Ethical Standard 1 (Revised): Code of Ethics for Assurance Practitioners issued by the New Zealand Auditing and Assurance Standards Board.

Other than in our capacity as auditor, 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

Finance and Performance Report

FOR THE YEAR ENDED 30 JUNE 2017

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 maintaining 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 2017.

Privacy Commissioner

J Edwards

25 October 2017

General Manager

G F Bulog

25 October 2017

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 2014-2018 identified five strategic initiatives to support the Office's strategic objective of promoting and protecting individual privacy. The Statement of Performance Expectations for the year to June 2017 identified four output classes to support these five initiatives as illustrated in figure one below.

The Office has recently published a new Statement of Intent for the period 1 July 2017- 30 June 2021 and so this will be the last report against these specific initiatives. Whilst the overall aim of the Office has remained unchanged in the new document, the reporting of performance will be against a new set of criteria from 2018.

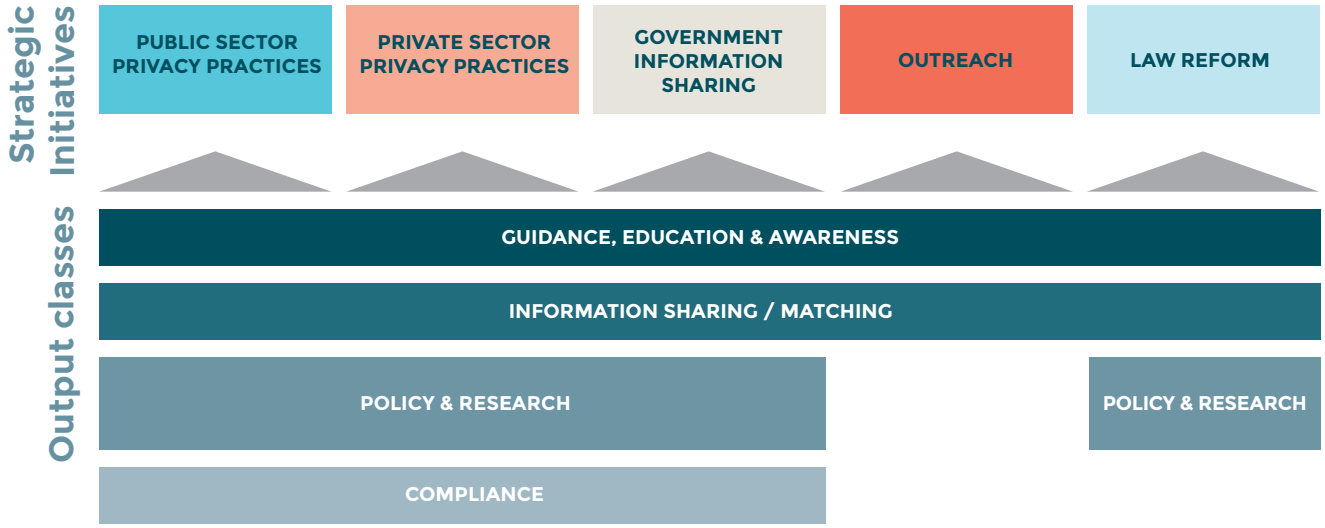


FIG 9: THE RELATIONSHIP BETWEEN OUTPUT CLASSES AND STRATEGIC INITIATIVES

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 for the year to June 2017.

PERFORMANCE AGAINST STRATEGIC INTENTIONS/INITIATIVES

STRATEGIC INITIATIVE	WHAT WE EXPECTED TO ACHIEVE BY JUNE 2017	HOW WE HAVE PERFORMED
Public sector privacy practices	Trust in government handling of personal information improves.	In 2016, the Office commissioned its seventh independent survey of New Zealanders' views on individual privacy and the handling of personal information. The last survey was completed in 2014. The survey identified that there has been an overall decrease in concern regarding the sharing of information by Health Organisations (a reduction of 6% to 47%) and Government Agencies (a reduction of 8% to 59%). Whilst the results above indicate increased levels of confidence in government handling of information, retaining this level of confidence and improving it remains a key area of focus for the Office.
Private sector privacy practices	Privacy by Design incorporated in the handling of personal information by private sector organisations.	The Office has undertaken a number of speaking engagements to private sector organisations throughout the year, including such major employers as Air New Zealand. An expanded range of e-learning modules has also been delivered. In May the Office launched the Employment and Privacy module which was developed to support private sector employers in the handling of personal information. In addition, the Office has been active in developing AskUs, and growing the range of answers offered in response to questions posed by individual users.
Government information sharing	Privacy breaches not a result of information sharing programmes.	During the year to 30 June 2017, the Office has received 132 voluntary notifications of privacy breaches. As previously reported, the majority of these breaches have been as a result of e-mail errors and not as a result of information sharing programmes. The Office continues to provide education and guidance in relation to information sharing programmes. In particular, towards the end of 2016 the Office launched the Trusted Sharing Consultancy Service. Through this, a number of agencies have been assisted to address a range of polices that have an information sharing component.
Outreach	Guidance and education materials available from the Privacy Commissioner and through third party providers	The Office continues to provide a variety of guidance and education tools on its website. While the website is the Office's main portal to share and disseminate information, hard copy guidance resources are still available and regional visits are regularly undertaken as part of the wider outreach programme. During the 2017 year, three new e-learning modules were launched – Credit Reporting and Privacy, Employment and Privacy, and Privacy ABC. There have been 498 registrations in total for these three modules since their launch. Registrations have been particularly strong for the short and accessible Privacy ABC. For the year ending 30 June 2017, 3,807 people registered for on-line training modules.
Law reform	Privacy Act incorporating changes passed into law Office incorporates law changes in its role as an effective regulator.	The new Privacy Bill is being drafted by the Parliamentary Counsel Office and the Privacy Commissioner has continued to provide ongoing support and advice to the Ministry of Justice. The Privacy Commissioner made six recommendations for further reform to the Act in his report on its operability under s 26 of the Act. The Intelligence and Security Act 2017 included amendments to the Privacy Act (not immediately in force). Work commenced on amendments to three Codes of Practice issued under the Privacy Act, to reflect amendments made to information privacy principle 11 under the Intelligence and Security Act 2017.

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	4,970	4,970
Other Revenue	221	199
Total Revenue	5,191	5,169

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 21.2% of the total Justice Advocacy, Advice and Promotion Services Appropriation for 2016/17. The total expenses in the year are $5,093k as set out in the Cost of Service Statement below.

As set out in the 2016/17 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 2016

	ACTUAL 2017 $000	BUDGET 2017 $000	ACTUAL 2016 $000
OUTPUT CLASS 1:			
Guidance, education and awareness			
Resources employed			
Revenue	742	758	790
Expenditure	635	689	734
Net Surplus(Deficit)	107	69	56
OUTPUT CLASS 2:			
Policy and Research			
Resources employed			
Revenue	2,038	2,088	1,911
Expenditure	2,062	2,147	2,179
Net Surplus(Deficit)	(24)	(59)	(268)
OUTPUT CLASS 3:			
Information Sharing/Matching			
Resources employed			
Revenue	775	646	867
Expenditure	680	539	822
Net Surplus(Deficit)	95	107	45
OUTPUT CLASS 4:			
Compliance			
Resources employed			
Revenue	1,614	1,699	1,713
Expenditure	1,716	1,874	1,900
Net Surplus(Deficit)	(102)	(175)	(187)
TOTALS:			
Resources employed			
Revenue	5,169	5,191	5,281
Expenditure	5,093	5,249	5,635
Net Surplus(Deficit)	76	(58)	(354)

The following tables set out assessment of the Office's performance against the targets as set out in the Statement of Performance Expectations. They also reflect the Justice Advocacy, Advice and Promotion appropriation. The following grading system has been used:

CRITERIA	RATING
On target or better	Achieved
< 5% away from target	Substantially achieved
>5% away from target	Not achieved

OUTPUT CLASS 1: GUIDANCE, EDUCATION AND AWARENESS

Why is this important?

One of the functions of the Privacy Commissioner is to promote individual privacy. Outreach to the public and businesses is a major focus and includes an active programme of seminars, presentations and regional outreach visits, as well as responding to enquiries from the public, media and businesses. The Office also produces a range of guidance and other resource material.

During the 2016/17 year, the website was increasingly used to provide such services online particularly through the provision of the on-line modules and Ask Us (on-line enquiries tool) which was launched at the end of 2016 financial year.

Output Measures

Quantity			
MEASURE	**ESTIMATE**	**ACHIEVED 2016/17**	**ACHIEVED 2015/16**
Number of people completing education modules on the new on-line system	2,500	Achieved 2,761 people have completed the Privacy 101, Health 101, PIA and Credit Reporting Privacy Code (CRPC) on-line modules in the year to 30 June 2017. (Completion has been assessed as those who have completed the post course quiz). In addition, there have been 52 registrations for the AISA module, 174 for the Employment module and 137 for the Privacy ABC module.	Substantially achieved
Presentations at conferences / seminars	90	Achieved 107 presentations completed in the year.	98
Public enquiries received and answered	7,500[1]	Significantly achieved – 7,320 This represents public enquiries received directly by the Office. Most of these were received by phone or e-mail. In addition, the Office received 8,433 enquiries through its interactive "Ask Us" on-line tool. This went live right at the end of June 2016.	7,783
Media enquiries received and answered	250	Not achieved – 217 This represents the number of media enquiries received by the Office. It is demand driven.	218

1 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 2016/17**	**ACHIEVED 2015/16**
Evaluations following on-line training indicate increased understanding by the participant in 80% of evaluations.	80%	Not achieved In the year to 30 June 2017, 34% have increased their understanding in the Privacy 101, Health 101, PIA and CRPC modules. A further 12% scored 100% in both the pre and post course tests. The test results are proxy and do not represent a pass/fail achievement. The Office expects that in many instances there would be only marginal differences between the score achieved before and after completion. These results do not reflect participation in all modules, as some are structured to have quizzes throughout the module.	Not Achieved – 45%
Website contains all current published guidance from the Privacy Commissioner, and additional resources to support compliance with the Act.	Achieved	Achieved	Achieved
The office actively engages with a wide range of stakeholders both nationally and internationally through our policy, dispute resolution and public affairs work.	Achieved	Achieved	Achieved
The percentage of respondents to the annual stakeholder survey who indicate, where applicable, that the guidance materials reviewed on the website were useful and met their needs.	85%	Achieved – 98%	Not reported – new measure
Provide advice and training to key stakeholders regarding information sharing to provide an understanding across the public sector of how information can be shared to achieve results and minimise risks, including the use of technology.	Achieved	Achieved In late 2016, the Office launched the Trusted Sharing Consultancy Service and through this has assisted agencies to address a range of policies that have an information sharing component. In addition, through its' programme of presentations, and its' on-line AISA training module, the Office has provided further guidance in this specific area.	Achieved

Timeliness			
MEASURE	**ESTIMATE**	**ACHIEVED 2016/17**	**ACHIEVED 2015/16**
Respond to all enquiries within 1 working day.	100%[2]	Not achieved – 93% The timeliness is likely to have been impacted by the earthquake in the latter half of 2016, resulting in the Wellington Office being vacated. The form in which enquiries are received has also changed. 2017 saw an increase in the proportion of enquiries being received by e-mail by 8% and an overall increase in e-mail enquiries from 2016 of 33%.	96%
Guidance materials are produced within agreed timelines as set out in the work plan.	Achieved	Achieved	Achieved

OUTPUT CLASS 2: POLICY AND RESEARCH

Why is this important?

The Privacy Commissioner actively comments and responds on legislative, policy or administrative proposals that impact on privacy to ensure that the requirements of the Privacy Act are being taken into account. Active

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

involvement in international fora also takes place and provides the Privacy Commissioner with the ability to identify and respond to emerging issues in a timely manner.

Output Measures

Quantity			
MEASURE	**ESTIMATE**	**ACHIEVED 2016/17**	**ACHIEVED 2015/16**
The number of the following pieces of work completed during the year:.		Achieved	Not reported – new measure
Proposals involving the use of personal information or other privacy issues, received for consultation or advice from the public and private sectors;	100	186	
Submissions and other formal reports, including submissions to select committees; and	15	22	
Office projects, including research projects.	10	15	
Identifiable progress in international efforts in which we are actively engaged to work towards more sustainable platforms for cross border co-operation.	Achieved	Achieved OPC efforts through the OECD, have furthered cooperation on international metrics in breach notification.	Achieved

Quality			
MEASURE	**ESTIMATE**	**ACHIEVED 2016/17**	**ACHIEVED 2015/16**
The percentage of recipients of policy advice who are satisfied with the service they received from the Privacy Commissioner.	85%[3]	Achieved – 93%	90%
Our participation in the law reform process is valued by the Ministry of Justice.	Achieved	Achieved Based on feedback we have received through discussions with the Ministry.	Achieved
The percentage of externally reviewed policy files that are rated 3.5 out of 5 or better for quality.	85%	Substantially achieved – 80% Based on findings from an independent review of a sample of policy files closed in the year. The assessment was undertaken in a way consistent with the assessment of technical quality that government departments with policy appropriations are required to report against. This is different to the methodology that was used in the prior year.	90%

Timeliness			
MEASURE	**ESTIMATE**	**ACHIEVED 2016/17**	**ACHIEVED 2015/16**
The percentage of policy files where advice was delivered within agreed timeframes.	100%	Significantly achieved – 96%	99%[4]
Requests for input into the law reform are made available within agreed timeframes.	90%	Achieved – 100%	100%

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

4 The prior year result is against a measure worded "Advice on proposals provided within agreed timeframes". The current year measure was re-worded to make it clearer.

OUTPUT CLASS 3: INFORMATION SHARING/MATCHING

Why is this important?

The Privacy Commissioner has statutory roles in overseeing authorised information matching programmes (Part 10 of the Privacy Act) and approved information sharing agreements (Part 9A of the Privacy Act). The Privacy Commissioner also provides advice to agencies carrying out information sharing and matching about how to meet their responsibilities under Part 9A and Part 10 respectively.

Output Measures

Quantity			
MEASURE	**ESTIMATE**	**ACHIEVED 2016/17**	**ACHIEVED 2015/16**
The number of information matching programmes monitored under Part 10 of the Privacy Act.	56[5]	Achieved – 56 There are 52 current programmes and 1 that ceased during the year. In addition, there are 3 programmes that were not operational during the year.	56
The number of new Approved Information Sharing Agreements received for consultation under s96(O) of the Privacy Act.	2	Achieved – 4	Not achieved
The number of formal reports produced that relate to information sharing or information matching programmes, under sections 96O, 96P, 96X or 106 of the Privacy Act.	8	Not achieved – 6 formal reports were produced. This is made up of 1 s106 report, 1 s96P report and 4 s96O reports. 3 of the s96O reports are also included in the figure above for consultations for new Information Sharing agreements.	Not reported – new measure
The number of proposals consulted on involving information sharing or matching between government agencies, completed during the year.	10	Achieved – 33	Not reported – new measure

Quality			
MEASURE	**ESTIMATE**	**ACHIEVED 2016/17**	**ACHIEVED 2015/16**
The percentage of recipients of information sharing and matching advice that are satisfied with the service they received from the Privacy Commissioner.	85%	Achieved – 95%	93%
The percentage of externally reviewed information sharing and matching files that are rated as 3.5 out of 5 or better for quality.	85%	Substantially achieved – 80% Based on findings from an independent review of a sample of Information Sharing and Matching files closed in the year. The assessment was undertaken in a way consistent with the assessment of technical quality that government departments with policy appropriations are required to report against.	Not reported – new measure

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

Timeliness			
MEASURE	**ESTIMATE**	**ACHIEVED 2016/17**	**ACHIEVED 2015/16**
The percentage of information sharing and matching files where advice was delivered within agreed timeframes.	100%	Substantially achieved – 98%	100%

OUTPUT CLASS 4: COMPLIANCE

Why is this important?

The provision and management of an independent, responsive, complaints and investigation process is another core function of the Office. The Office continues to transform the way in which it deals with complaints with a focus on more timely resolution. Back in the 2014/15 year the Office introduced an online complaints lodgement system. In the year to 30 June 2017 approximately 46% of complaints were being lodged in this way.

In addition, the Office also reviews and amends codes of practice.

Output Measures

Quantity			
MEASURE	**ESTIMATE**	**ACHIEVED2016/17**	**ACHIEVED 2015/16**
Number of complaints received	900[6]	Not achieved – 736 complaints received	969
Number of data breach notifications received.	100	Achieved – 132 notifications received 79 of these related to public sector organisations and 53 related to private sector organisations.	Not reported – new measure

Quality			
MEASURE	**ESTIMATE**	**ACHIEVED 2016/17**	**ACHIEVED 2015/16**
The percentage of complainants' and respondents' who rate their satisfaction with the complaints handling process as "satisfactory" or better.	65%[6]	Not achieved – 43% There were a total of 168 responses to the survey. 33% of complainants reported being satisfied with the complaints handling process compared to 76% of respondents. The impact of the earthquake meant the Office's ability to communicate easily with complainants was impeded for two to three months of the year. The process was run internally in the current year which differs to the external process run in 2016. Similar questions were asked in each survey to ensure a level of comparability. A review of the results will be undertaken by the Office and the survey process itself will be an area of focus over 2017/18.	52%
The percentage of complaints files closed by settlement between the parties.	40%[6]	Achieved – 48%	49%
Amendments to codes of practice meet all statutory requirements.	100%	Achieved Statutory requirements were met for the January 2017 amendment to the Telecommunications Information Privacy Code.	100%
The percentage of externally reviewed complaints investigations that are rated as 3.5 out of 5 or better for quality.	85%[6]	Achieved – 100%	94%

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

Timeliness			
MEASURE	**ESTIMATE**	**ACHIEVED 2016/17**	**ACHIEVED 2015/16**
The percentage of open files greater than 6 months old at the year end.	10%[7]	Achieved – 10% This represents a total of 26 files out of 253 files that were open at the year-end.	8.7%
Review of the operation of Credit Reporting Code substantially progressed.	Achieved	Achieved Substantial progress was made during the year in analysing submissions on the review. The report will be completed in the next financial year.	Not achieved.

STATEMENT OF ACCOUNTING POLICIES

FOR THE YEAR ENDED 30 JUNE 2017

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 requirements of the Crown Entities Act 2004.

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 2017, and were approved by the Commissioner on 25 October 2017. 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.

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.

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

Summary of Significant Accounting Policies

Significant accounting policies are included in the notes to which they relate.

Significant accounting policies that do not relate to specific notes are outlined below.

Budget figures

The budget figures are derived fron the statement of performance expectations as 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.

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.

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.

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:

- Useful lives and residual values of property, plant and equipment – refer to Note 9
- Useful lives of Software assets – refer to 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 2017:

- Lease classification – refer Note 4
- Non-Government Grants – refer Note 2
- Grant Expenditure – refer Note 4

STATEMENT OF COMPREHENSIVE REVENUE AND EXPENSES

FOR THE YEAR ENDED 30 JUNE 2017

	NOTE	ACTUAL 2017 $000	BUDGET 2017 $000	ACTUAL 2016 $000
Revenue				
Crown Revenue	2	4,970	4,970	4,970
Other revenue	2	199	221	311
Total Income		5,169	5,191	5,281
Expenditure				
Promotion	4	55	68	98
Audit Fees		30	29	29
Depreciation and Amortisation	4,9,10	185	222	183
Rental Expenses		411	410	400
Operating Expenses		621	694	825
Contract Services		84	100	298
Staff Expenses	3	3,707	3,726	3,802
Total Expenditure		5,093	5,249	5,635
Surplus/ (Deficit)		76	(58)	(354)
Other comprehensive revenue and expenses		-	-	-
Total comprehensive revenue and expenses		**76**	**(58)**	**(354)**

STATEMENT OF CHANGES IN EQUITY

FOR THE YEAR ENDED 30 JUNE 2017

	NOTE	ACTUAL 2017 $000	BUDGET 2017 $000	ACTUAL 2016 $000
Total Equity at the start of the year		1,043	1,188	1,397
Total comprehensive revenue and expenses for the year		**76**	**(58)**	**(354)**
Total Equity at the end of the year	**5**	**1,119**	**1,130**	**1,043**

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 2017

	NOTE	ACTUAL 2017 $000	BUDGET 2017 $000	ACTUAL 2016 $000
Public Equity				
General funds	5	1,119	1,130	1,043
Total public equity		**1,119**	**1,130**	**1,043**
Current assets				
Cash & cash equivalents	6	994	1,080	885
Receivables	7	35	44	42
Inventory	8	18	23	22
Prepayments	7	67	12	29
Total Current Assets		1,114	**1,159**	978
Non-current assets				
Property, Plant & Equipment	9	320	412	419
Intangible assets	10	148		164
Total non-current assets		468	412	583
Total assets		**1,582**	**1,571**	**1,561**
Current liabilities				
Payables	11	165	163	234
Employee entitlements	13	246	225	213
Total current liabilities		411	388	447
Non-current liabilities				
Lease incentive	12	52	53	71
Total non-current liabilities		52	53	71
Total Liabilities		**463**	**441**	**518**
Net assets		**1,119**	**1,130**	**1,043**

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

STATEMENT OF CASH FLOWS

FOR THE YEAR ENDED 30 JUNE 2017

	ACTUAL 2017 $000	BUDGET 2017 $000	ACTUAL 2016 $000
Cash flows from operating activities			
Cash was provided from:			
Receipts from the Crown	4,970	4,970	4,970
Receipts from other revenue	190	173	263
Interest received	35	48	49
Cash was applied to:			
Payment to suppliers	1,335	1,325	1,648
Payments to employees	3,689	3,726	3,727
Net Goods and Services Tax	(8)	(4)	(10)
Net cash flows from operating activities	**179**	**144**	**(83)**
Cash flows from investing activities			
Cash was applied to:			
Purchase of Property Plant and Equipment and Intangibles	70	145	84
Net cash flows from investing activities			
Net increase (decrease) in cash held	109	(1)	(167)
Plus opening cash	885	1,081	1,052
Closing cash balance	994	1,080	885
Cash and bank	**994**	**1,080**	**885**

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 2017

NOTE 1: EXPLANATION OF MAJOR VARIANCES AGAINST BUDGET

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 reported surplus is significantly different to the budgeted deficit of $58k. This is primarily due to the following:

Operating expenses (down on budget by $73k)

There has been reduced expenditure in a number of areas but most notably in the areas of staff travel, other staff costs and litigation costs. These account for a $79k reduction against budget.

Depreciation expense (down on budget by $37k)

The cost of additions during the year has been less than budgeted resulting in a lower than anticipated depreciation expense.

NOTE 2: REVENUE

Accounting Policy

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 revenue is recognised by accruing on a time proportion basis.

Sale of publications

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

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.

Critical judgements in applying accounting policies

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. In the current year, no new grants have been awarded.

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 (2016: $nil).

Other revenue breakdown

	ACTUAL 2017 $000	ACTUAL 2016 $000
Other grants received	161	206
Rental income from property sub-leases	-	10
Privacy Forum	-	34
Seminars & Workshops	3	12
Interest revenue	35	49
Other	-	-
Total other revenue	**199**	**311**

NOTE 3: STAFF EXPENSES

Accounting Policy

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.

Breakdown of staff costs and further information

	ACTUAL 2017 $000	ACTUAL 2016 $000
Salaries and wages	3,544	3,590
Employer contributions to defined contribution plans	105	105
Other Staff expenses	25	32
Increase/(decrease) in employee entitlements	33	75
Total Staff Expenses	**3,707**	**3,802**

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 2017	ACTUAL 2016
$100,000 – $109,999	2	1
$110,000 – $119,999	2	2
$120,000 – $129,999		
$130,000 – $139,999	1	1
$140,000 – $149,999		
$150,000 – $159,999	1	
$160,000 – $169,999	1	1
$170,000 – $179,999		
$180,000-$189,999	2	1
$190,000-$199,999		1
$310,000-$319,999		1
$320,000-$329,999	1	

No redundancy payments were made in the year. (2016: $Nil)

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

Commissioner's Total Remuneration

In accordance with the disclosure requirements of Section 152 (1) (a) of the Crown Entities Act 2004, the total remuneration includes all benefits paid during the period 1 July 2016 to 30 June 2017.

NAME	POSITION	AMOUNT 2017	AMOUNT 2016
John Edwards	Privacy Commissioner	321,894	318,603

NOTE 4: OTHER EXPENSES

Accounting Policy

Operating leases

Operating lease expenses are recognised on a straight-line basis over the term of the lease.

Grant Expenditure

Discretionary grants are those grants where the Office of the Privacy Commissioner has no obligation to award the grant on receipt of the grant application. Discretionary grants with substantive conditions are expensed when the grant conditions have been satisfied.

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.

Critical judgements in applying accounting policies

Grant Expenditure

During the previous financial year, the Privacy Commissioner approved 4 discretionary grants under its Privacy Good Research Fund with the aim of stimulating privacy related research by external entities. No further grants were approved in the 2017 year. The conditions included milestones and specific requirements. The Office of the Privacy Commissioner has accounted for the related grant expenses when evidence of meeting these milestones has been received from the recipient.

A total of $64k was expensed in relation to these grants in 2016 and a further $12k was expensed in 2017.

Lease Classification

Determining whether a lease is to be treated as an operating lease or a finance lease requires some judgement. Leases where the lessor effectively retains substantially all the risks and benefits of ownership of the leased items are classified as operating leases.

Other expenses and further information

The total comprehensive revenue and expenses is after charging for the following significant expenses:

	ACTUAL 2017 $000	ACTUAL 2016 $000
Fees paid to auditors:		
External audit – Current Year	30	29
Promotion costs:		
Website development expenses	32	44
Privacy Forum	7	35
Other marketing expenses	16	19
Total promotion expenses	**55**	**98**
Depreciation and amortisation:		
Furniture & Fittings	72	73
Computer Equipment	34	58
Office Equipment	6	10
Intangibles	73	42
Total depreciation and amortisation	**185**	**183**
Rental expense on operating leases	411	400
Contract Services	82	298
Other operating expenses:		
Computer maintenance/licenses	138	156
Staff travel	131	145
Staff Development	33	72
Loss on disposal of assets	-	14
Grant expenditure	12	64
Research related	14	20
Recruitment	30	70
Litigation	-	27
Utilities	79	82
Other	184	175
Total other operating expenses	**621**	**825**

Operating leases as lessee

The future aggregate minimum lease payments to be paid under non-cancellable leases are as follows:

	ACTUAL 2017 $000	ACTUAL 2016 $000
Not later than one year	382	370
Later than one year and not later than five years	830	1,157
Later than five years	-	-
Total non-cancellable operating leases	**1,212**	**1,527**

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

The Privacy Commissioner leases two properties, one in Wellington and the other in Auckland. The Wellington lease was re-negotiated in 2015 and will expire in February 2021. A lease incentive was offered as part of the negotiation. This is accounted for in line with PBE IPSAS 13 Leases.

The property in Auckland was sublet in part up until December 2015, due to it being surplus to requirements. Notice was given to the current tenants and this space is now utilised by the Office. The lease on the Auckland premises will expire on 31 July 2019.

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

There are no restrictions placed on the Privacy Commissioner by any of its leasing arrangements.

NOTE 5: GENERAL FUNDS

	ACTUAL 2017 $000	ACTUAL 2016 $000
Opening balance	1,043	1,397
Net (deficit) / surplus	76	(354)
Closing balance	**1,119**	**1,043**

NOTE 6: CASH AND CASH EQUIVALENTS

Accounting Policy

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.

	ACTUAL 2017 $000	ACTUAL 2016 $000
Cash on hand and at bank	32	9
Cash equivalents – on call account	962	876
Total cash and cash equivalents	**994**	**885**

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

NOTE 7: RECEIVABLES

Accounting Policy

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.

	ACTUAL 2017 $000	ACTUAL 2016 $000
Receivables	35	42
Prepayments	67	29
Total	**102**	**71**

Total receivables comprise:

GST receivable (exchange transaction)	34	41
Other receivables (non-exchange)	1	1
	35	**42**

The carrying value of receivables approximates their fair value.

The carrying amount of receivables that would otherwise be past due, but not impaired, whose terms have been renegotiated is $NIL (2016: $NIL).

NOTE 8: INVENTORIES

Accounting Policy

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.

	ACTUAL 2017 $000	ACTUAL 2016 $000
Publications held for sale	1	3
Publications held for distribution	17	19
Total Inventories	**18**	**22**

No inventories are pledged as security for liabilities (2016: $NIL) and no inventories were written down. (2016: $NIL).

NOTE 9: PROPERTY, PLANT AND EQUIPMENT

Accounting Policy

Property, plant and equipment asset classes consist of Furniture and Fittings, Computer Equipment and Office Equipment.

Property, plant and equipment are shown at cost 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.

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.

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.

Impairment of Property, Plant and Equipment

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.

Critical accounting estimates and assumptions

Estimating useful lives and residual values of property, plant and equipment

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.

Breakdown of property, plant and equipment and further information

	FURNITURE AND FITTINGS $000	COMPUTER EQUIPMENT $000	OFFICE EQUIPMENT $000	TOTAL $000
Cost				
Balance at 1 July 2015	**715**	**305**	**59**	**1,079**
Additions	1	20	0	21
Disposals	(1)	(5)	0	(6)
Balance at 30 June 2016	**715**	**320**	**59**	**1,094**
Balance at 1 July 2016	**715**	**320**	**59**	**1,094**
Additions	0	13	0	13
Disposals	0	(6)	0	(6)
Balance at 30 June 2017	**715**	**327**	**59**	**1,101**
Accumulated depreciation and impairment losses				
Balance at 1 July 2015	**323**	**185**	**32**	**540**
Depreciation expense	73	58	10	141
Disposals	(1)	(5)	-	(6)
Balance at 30 June 2016	**395**	**238**	**42**	**675**
Balance at 1 July 2016	**395**	**238**	**42**	**675**
Depreciation expense	72	34	6	112
Elimination on disposal	0	(6)	0	(6)
Balance at 30 June 2017	**467**	**266**	**48**	**781**
Carrying amounts				
At 30 June and 1 July 2016	**320**	**82**	**17**	**419**
At 30 June 2017	**248**	**61**	**11**	**320**

Capital commitments

The Privacy Commissioner has capital commitments of $nil for the year 2016/17 (2016: $NIL).

NOTE 10: INTANGIBLE ASSETS

Accounting Policy

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.

Website Costs

Costs that are directly associated with the development of interactive aspects of the Office's website are capitalised when they are ready for use.

Costs associated with general maintenance and development of non-interactive aspects of the Office's website are recognised as an expense as 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 the 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	2-4 years	50%-25%
Interactive tools	3 Years	33.3%

The software is amortised over the length of the license. Some of these only have a 2 year life.

Impairment

Refer to the policy for impairment of property, plant and equipment in Note 9. The same approach applies to the impairment of intangible assets.

Critical accounting estimates and assumptions

Estimating useful lives of software assets

The Office's interactive website tools comprise of two interactive databases that went live in mid-2016 and 3 new interactive e-learning tools developed in 2017. Both tools were developed by an external provider. These tools have a finite life, which requires the Office to estimate the useful life of the assets.

In assessing the useful lives of these tools, a number of factors are considered, including:

- The effect of technological change on systems and platforms; and
- The expected timeframe for the development of replacement systems and platforms.

An incorrect estimate of the useful lives of these assets will affect the amortisation expense recognised in the surplus or deficit, and the carrying amount of the assets in the statement of financial position.

Taking the above into account the Office has estimated a useful life of 3 years for these interactive tools and there are currently no indicators that the period of use of the tools will be materially different.

Movements for each class of intangible asset are as follows:

	ACQUIRED SOFTWARE $000	INTERACTIVE TOOLS $000	TOTAL $'000
Cost			
Balance at 1 July 2015	106	-	106
Additions	36	147	183
Disposals	(34)	-	(34)
Balance at 30 June 2016	**108**	**147**	**255**
Balance at 1 July 2016	108	147	255
Additions	-	57	57
Disposals	-	-	-
Balance at 30 June 2017	108	204	312
Accumulated amortisation and impairment losses			
Balance at 1 July 2015	69	-	69
Amortisation expense	31	11	42
Disposals	(20)	-	(20)
Balance at 30 June 2016	80	11	91
Balance at 1 July 2016	80	11	91
Amortisation expense	18	55	73
Disposals	-	-	-
Balance at 30 June 2017	**98**	**66**	**164**
Carrying amounts			
At 30 June and 1 July 2016	28	136	164
At 30 June 2017	**10**	**138**	**148**

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

Capital commitments

The Privacy Commissioner has capital commitments of $26K for the development of interactive tools (2016: $16K).

NOTE 11: PAYABLES

Accounting Policy

Creditors and other payables are recorded at the amount payable.

Breakdown of payables

	ACTUAL 2017 $000	ACTUAL 2016 $000
Payables under exchange transactions		
Creditors	43	115
Accrued expenses	76	99
Lease incentive	20	20
Income received in advance	26	-
Total payables under exchange transactions	165	234
Payables under non-exchange transactions		
Other payables (GST)	-	-
Total payables under non-exchange transactions	-	-
Total creditors and other payables	**165**	**234**

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 12: NON-CURRENT LIABILITIES

	ACTUAL 2017 $000	ACTUAL 2016 $000
Lease incentive	52	71
Total non-current liabilities	52	71

Lease incentive for the Wellington office for the period 23 February 2015 to 22 February 2021 (6 year lease).

NOTE 13: EMPLOYEE ENTITLEMENTS

Accounting policy

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.

Breakdown of employee entitlements

	ACTUAL 2017 $000	ACTUAL 2016 $000
Current employee entitlements are represented by:		
Accrued salaries and wages	68	60
Annual leave	178	153
Total current portion	**246**	**213**
Current	246	213
Non-current	-	-
Total employee entitlements	**246**	**213**

NOTE 14: 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 (2016: $nil).

NOTE 15: RELATED PARTY INFORMATION

The Privacy Commissioner is a wholly owned entity of the Crown. The Government significantly influences the role of the Privacy Commissioner as well as being its major source of revenue.

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 2017 $000	ACTUAL 2016 $000
Total Salaries and other short-term employee benefits	1,125	1,057
Full-time equivalent members	6	5.5

Key management personnel include all Senior Managers and the Privacy Commissioner who together comprise the Senior Leadership Team (SLT). There have been no changes in the composition of the SLT during the year.

NOTE 16: 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 17: FINANCIAL INSTRUMENTS

17A Financial instrument categories

The carrying amounts of financial assets and liabilities in each of the financial instrument categories are as follows:

	2017 $000	2016 $000
FINANCIAL ASSETS		
Loans and Receivables		
Cash and cash equivalents	994	885
Receivables (excluding prepayments and taxes receivables)	1	1
Total loans and receivables	**995**	**886**
FINANCIAL LIABILITIES		
Financial liabilities at amortised cost		
Payables (excluding income in advance, taxes payable, grants received subject to conditions and lease incentive)	119	214
Total financial liabilities at amortised cost	**119**	**214**

Appendix A – Processes and Services

Investigations

Our investigations team forms the regulatory 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 access or correction of information.

During the course of an investigation we determine the following:

- Whether a situation is covered under the Privacy Act
- Whether the respondent agency is responsible
- The level of harm caused by the breach

We try to reach a settlement of the complaint 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 a case to the Director of Human Rights Proceedings, who may choose to bring a case in front of the Human Rights Review Tribunal. We do not always refer cases. We will be likely to refer particularly serious cases, or cases 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 take a case that we refer, the complainant still has the option of taking the respondent to the Tribunal on his/her 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. However, our views and findings are taken seriously.

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 Approved Information Sharing Agreements (AISAs). These are agreements between government agencies that allow them to share information with one another. 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 'automate away' 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
- Our fortnightly 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 programmes' compliance in the following manner. There are three levels:

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

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 2 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)/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.	✓
6. 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.	✓
7. 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).	✓
8. BDM(Deaths)/INZ Deceased Temporary Visa Holders To identify and remove or update the records of people who are deceased from the Immigration New Zealand (INZ) database of overstayers and temporary permit holders. BDM disclosure to INZ: BDM provides information from the Deaths Register covering the six months prior to the extract date. The information includes full name at birth, full name at death, gender, birth date, death date, country of birth, and number of years lived in New Zealand.	✓
9. BDM(Deaths)/IR Deceased Taxpayers To identify taxpayers who have died so that IR can close accounts where activity has ceased. BDM disclosure to IR: BDM provides death information including the full name, gender, birth date, death date, home address, death registration number and spouse's details.	✓
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 extract date. The death details include the full name (current and at birth), gender, date and place of birth, date of death, home address and death registration number.	✓
14. BDM(Marriages)/MSD Married Persons To identify current clients who have married so that MSD can update client records and reassess their eligibility for benefits and allowances. BDM disclosure to MSD: BDM provides marriage information covering the week prior to the extraction date. The marriage details include the full names of each spouse (including name at birth if different from current name), their birth dates and addresses, and registration and marriage dates.	✓
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/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.	✓
CITIZENSHIP ACT 1977, S.26A	
	COMPLIANCE
18. 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.	✓
19. 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.	✓
20. Citizenship/INZ Entitlement to Reside To remove from the Immigration New Zealand (INZ) overstayer records the names of people who have been granted New Zealand citizenship. Citizenship disclosure to INZ: Citizenship provides information from the Citizenship Register about people who have been granted citizenship. Each record includes full name, gender, date of birth, country of birth and citizenship person number.	✓

CORRECTIONS ACT 2004, S.180	
	COMPLIANCE
21. 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
22. 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
23. 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.	✓

CUSTOMS AND EXCISE ACT 1996, S.280B	
	COMPLIANCE
24. 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.	✓

CUSTOMS AND EXCISE ACT 1996, S.280D	
	COMPLIANCE
25. 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 the '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.	✓

CUSTOMS AND EXCISE ACT 1996, S.280H	COMPLIANCE
26. 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.	✓
27. 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).	✓

CUSTOMS AND EXCISE ACT 1996, S.280K	COMPLIANCE
28. 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).	✓

EDUCATION ACT 1989, S.226A AND S.235F	COMPLIANCE
29. 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
30. 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 date, end date (date of request), known education provider(s) used by this student and student ID number. MoE disclosure to MSD StudyLink: MoE returns to StudyLink information showing all providers and courses used by the student, course dates, course equivalent full-time student rating and course completion code.	✓

EDUCATION ACT 1989, S.360	
	COMPLIANCE
31. MoE/Education Council Registration To ensure teachers are correctly registered (Education Council) and paid correctly (Ministry of Education). MoE disclosure to Education Council: MoE provides full names, date of birth, gender, address, school(s) employed at, number of ½ days worked, registration number (if known), and MoE employee number. Education Council disclosure to MoE: The Education Council provides full names, date of birth, gender, address, registration number, registration expiry date, registration classification and MoE employee number (if confirmed).	✓
ELECTORAL ACT 1993, S.263A	
	COMPLIANCE
32. INZ/EC Unqualified Voters To identify, from immigration records, those on the electoral roll who appear not to meet New Zealand residence requirements, so their names may be removed from the roll. INZ disclosure to EC: Immigration New Zealand provides full names (including aliases), date of birth, address and permit expiry date. The type of permit can be identified because five separate files are received, each relating to a different permit type.	✓
ELECTORAL ACT 1993, 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: Citizenship provides full name, date of birth and residential address of new citizens aged 17 years and over (by grant or by descent).	✓
34. MSD/EC Unenrolled Voters To compare MSD's beneficiary and student databases with the electoral roll to: · identify beneficiaries and students who are qualified to vote but who have not enrolled so that they may be invited to enrol · update the addresses of people whose names are already on the roll. MSD disclosure to Electoral Commission: MSD provides full name, date of birth and address of all individuals aged 17 years or older for whom new records have been created or where key data (surname, given name or address) has changed, provided these records have not been flagged as confidential.	✓
35. NZTA(Driver Licence)/EC Unenrolled Voters To compare the driver licence register with the electoral roll to: · identify people who are qualified to vote but have not enrolled, so that they may be invited to enrol · update the addresses of people whose names are already on the roll. NZTA disclosure to Electoral Commission: NZTA provides the full name, date of birth and address of driver licence holders aged 17 and over whose records have not been marked confidential.	✓
36. NZTA(Vehicle Registration)/EC Unenrolled Voters To compare the motor vehicle register with the electoral roll to: · identify people who are qualified to vote but have not enrolled, so that they may be invited to enrol · update the addresses of people whose names are already on the roll. NZTA disclosure to Electoral Commission: NZTA provides the full names, date of birth and addresses of individuals aged 17 and over who registered a vehicle or updated their details in the period covered by the extract. The 'Owner ID' reference number is also included to identify any multiple records for the same person.	✓
37. DIA(Passports)/EC Unenrolled Voters To compare passport records with the electoral roll to: · identify people who are qualified to vote but have not enrolled so that they may be invited to enrol · update the addresses of people whose names are already on the roll. DIA (Passports) disclosure to Electoral Commission: Passports provides full name, date of birth and residential address of passport holders aged 17 years and over.	✓

ELECTRONIC IDENTITY VERIFICATION ACT 2012, S.39	
	COMPLIANCE
38. 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: Child's names, gender, birth date and birth place and country, citizenship by birth status, marriage date, registration number, mother's names, father's names, since died indicator and still born indicator. Deaths disclosure to IVS: Names, gender, date of birth, place of birth, date of death, place of death and age at death. Marriages disclosure to IVS: Names, date of birth, date of marriage, registration number, country of birth, gender, place of marriage, spouse's names. Citizenship disclosure to IVS: Names, gender, birth date, birth place, photograph, citizenship person identifier, citizenship certificate number, certificate type and certificate status. Passports disclosure to IVS: Names, gender, date of birth, place of birth, photograph, passport person identifier, passport number, date passport issued, date passport expired and passport status. Immigration disclosure to IVS: Whether a match is found, client ID number and any of the pre-defined set of identity related alerts.	✓

IMMIGRATION ACT 2009, S.295	
	COMPLIANCE
39. 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
40. 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 and start and expiry dates, and dates the person entered or left New Zealand. INZ may also disclose details of a parent or guardian of a young person.	✓

MOTOR VEHICLE SALES ACT 2003, S.122 AND S.123	
	COMPLIANCE
41. 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 match runs.	✓

SOCIAL SECURITY ACT 1964, S.126A	
	COMPLIANCE
42. MSD/Justice Fines Defaulters Tracing To enable the Ministry of Justice to locate people who have outstanding fines in order to enforce payment. Justice disclosure to MSD: Justice selects fines defaulters for whom it has been unable to find a current address from other sources (including the IR/Justice Fines Defaulters Tracing Programme), and sends the full name, date of birth and a data matching reference number to MSD. MSD disclosure to Justice: For matched records, MSD returns the last known residential address, postal address, residential, cell-phone and work phone numbers, and the unique identifier originally provided by Justice.	✓

SOCIAL SECURITY ACT 1964, S.126AC	
	COMPLIANCE
43. 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	
	COMPLIANCE
44. Australia (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
45. 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	
	COMPLIANCE
46. 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.	✓
47. 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.	✓
TAX ADMINISTRATION ACT 1994, S.82	
	COMPLIANCE
48. 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. Not compliant – substantive issue: MSD extended the selection, beyond the criteria in the authorising legislation, to include people with debts. A limited number of people were affected and MSD ceased this when challenged by IR. This match is replaced by an Approved Information Sharing Agreement from 31 August 2017.	X
49. 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
50. 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
51. 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.85A	
	COMPLIANCE
52. 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.	✓

TAX ADMINISTRATION ACT 1994, S.85G	
	COMPLIANCE
53. 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 in section 103(1B) of the Act as it does not advise individuals that they have 5 working days to challenge the suspension. We remain satisfied with the safeguards that IR has in place to address instances of incorrectly ceased entitlements. This match is replaced by an Approved Information Sharing Agreement from 31 August 2017.	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.

USER AGENCY PROGRAMME NAME APPROVAL DATE	REASON	GROUNDS
DEPARTMENT OF INTERNAL AFFAIRS		
Citizenship by Birth 30 March 2017	Efficiency and security	Satisfactory audit result
DIA – IDENTITY VERIFICATION SERVICE		
Identity verification (Births, Deaths & Marriages) 30 March 2017	Efficiency, transfer within agency	Satisfactory audit result
Identity verification (Citizenship) 30 March 2017	Efficiency, transfer within agency	Satisfactory audit result
Identity verification (Passports) 30 March 2017	Efficiency, transfer within agency	Satisfactory audit result
ELECTORAL COMMISSION		
Unqualified Voters 16 September 2016	Efficiency and data quality	Satisfactory audit result
INLAND REVENUE DEPARTMENT		
Child Support Alerts 4 August 2016	Efficiency and security	Timely delivery of data
MINISTRY OF JUSTICE		
Fines Defaulters Tracing (Customs) 11August 2016	Timely delivery of data	Audit issues scheduled for completion
MINISTRY OF SOCIAL DEVELOPMENT		
Australia Change in Circumstances 20 January 2017	Efficiency and security	Satisfactory audit result
Periods of Residence 20 January 2017	Efficiency and security	Satisfactory audit result
Verification of Study 30 June 2017	Efficiency and security	Timely delivery of data
Results of Study 30 June 2017	Efficiency and security	Timely delivery of data

Privacy Commissioner
Te Mana Matapono Matatapu