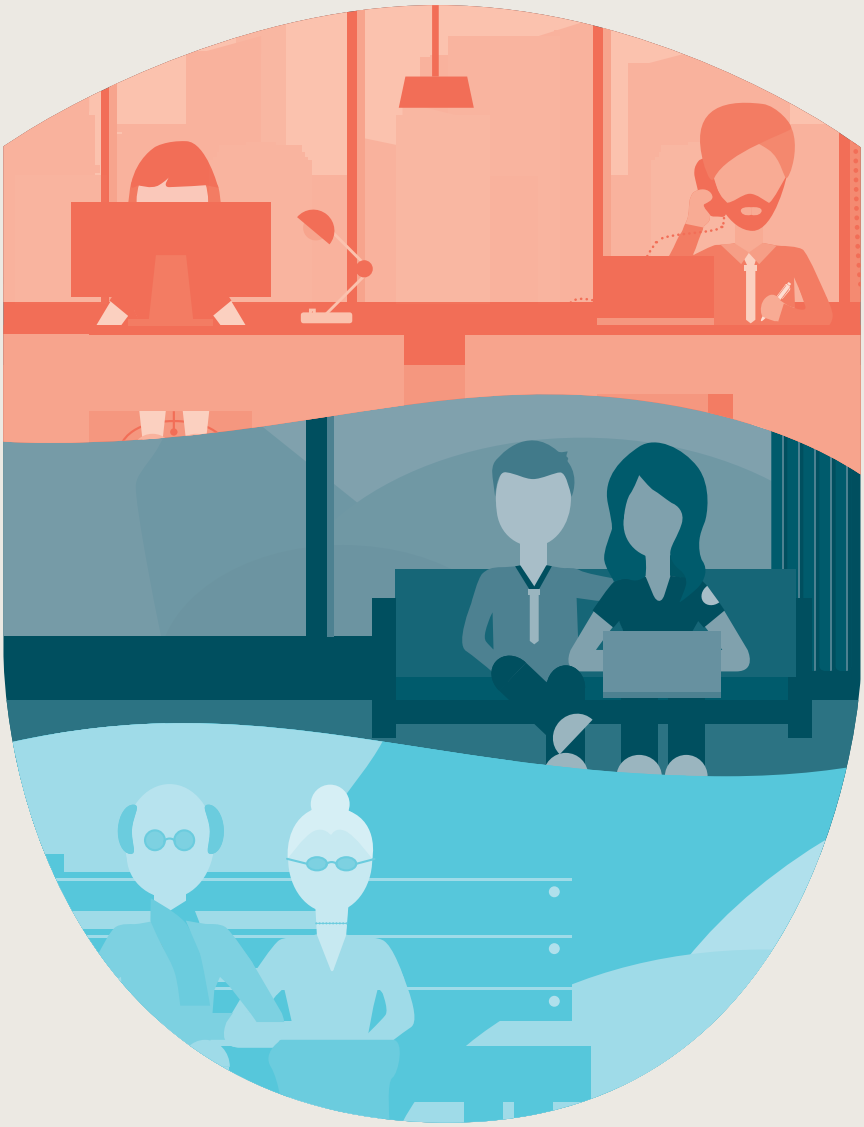
PRIVACY COMMISSIONER

Annual Report 2018



Privacy Commissioner
Te Mana Mātāpono Matatapu

Annual Report of the Privacy Commissioner

for the year ended 30 June 2018

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

The Minister of Justice

I tender my report as Privacy Commissioner for the year ended 30 June 2018

John Edwards
Privacy Commissioner
November 2018

Introduction

This year has seen dramatic changes to the way the privacy of personal information is regulated. Jurisdictions around the world have ushered in stronger privacy protections for their citizens in response to the increased role data processing has on our everyday lives.

At the same time, there has been an unprecedented level of media and public focus on privacy issues. New technologies and data breaches have prompted public discussion and led to a greater interest in privacy rights.

In amongst all of this, New Zealand is advancing its own privacy law reform. The Privacy Bill presents a unique opportunity to safeguard the rights of New Zealanders and catch up with advancing privacy legislation around the world.

A year of upheaval

The European Union's General Data Protection Regulation (GDPR) came into force in May 2018. It created one coherent data protection framework across the EU, and introduced significant penalties for non-compliance. The GDPR has set a high standard for data protection laws around the world. The law can also apply to agencies outside of the EU, which has made New Zealand business sit up and take notice.

In February 2018, Australia introduced mandatory data breach reporting. Agencies are now required to report breaches of personal information to regulators and sometimes victims.

In June 2018 California, the fifth largest economy in the world, passed a law which approximates the high tide mark of data protection internationally.

In that same month, the EU formally recognised the adequacy of Japan's data protection laws. Japan's new adequacy status also formed the core of a free trade agreement. New Zealand has enjoyed adequacy status with the EU since 2012.

These developments signal a growing trend in privacy law reform. New Zealand's law is no longer a leader in the privacy space like it was when Parliament first passed the Privacy Act 25 years ago.

In the public eye

According to the results of our most recent public opinion survey (released May 2018), more than half of all New Zealanders are more concerned about their individual privacy now than they were in the last few years.

This coincides with a series of incidents that have pushed privacy to the forefront of people's minds. The enactment of the GDPR led to floods of emails from companies alerting customers and users to updates in privacy policies.

Media reports on facial recognition, drones, and AI have triggered public debate about new technology and the implications it has for personal privacy.

Several prominent data breaches also made the headlines. One notable incident involved UK company Cambridge Analytica profiling voters using data harvested from 87 million Facebook users without permission. The revelations sparked outrage from users, and both the US Congress and European Parliament summoned Facebook to testify.

A long-expected law reform

In the midst of these international developments and privacy scandals, New Zealand's Privacy Bill was introduced to Parliament in March 2018.

During this reporting year we applied considerable resources to working with officials from the Ministry of Justice, and writing an extensive submission on the Bill.

We are pleased to see this reform taking its first steps. It moves us towards alignment with our international peers by introducing mandatory data breach reporting, new offences, increased fines, and other provisions.

However, the Bill as currently drafted does not go far enough. If the Bill passes in the state it entered the House, it will be a privacy law fit for 2013. We need to account for advances in technology, introduce meaningful consequences for non-compliance, and align with international best practice in a way that suits New Zealand's unique society.

We provided our submission on the Bill to the Justice Select Committee in May 2018. We recommended:

- civil penalties
- improved agency accountability for compliance
- personal information portability
- protections against re-identification
- letting the Commissioner decide which cases are to proceed to the Human Rights Review Tribunal and act as the plaintiff in those cases
- enhancing the existing privacy principles to provide an effective right to erasure
- algorithmic transparency and the right to object to automated processing.

We believe these changes will help future-proof our privacy law for the next 25 years and beyond.

Key points

Law reform

- The Privacy Bill was a major focus during the year, and we supported the Ministry of Justice with independent policy and drafting advice.
- We made a comprehensive submission to the Select Committee suggesting improvements to the Bill.

Dispute resolution

- We closed 706 investigation files.
- At the end of the reporting year, 89.1% of open investigation files were less than six months old.
- We continue to have regular external reviews of our investigations. This year the reviewer gave 95% of investigations assessed a score of 3.5 or higher.
- We referred five cases to the Director of Human Rights Proceedings.
- Twenty-nine complainants took proceedings to the Human Rights Review Tribunal themselves.
- We named one agency for non-compliance with the Privacy Act under our naming policy.

Codes of practice

- We amended three codes to reflect changes that the Intelligence and Security Act 2017 made to the Privacy Act.
- We completed a review of the comprehensive credit reporting system regulated by the Credit Reporting Privacy Code.

Policy

- We advised on 107 policy proposals that involved personal information.
- We published 14 submissions and formal reports.
- We collaborated with the Government Chief Data Steward to develop principles for safe and effective data analytics.

Outreach

- We hosted our biannual Privacy Forum at Te Papa Tongarewa. The full day forum attracted over 300 attendees from across the economy.
- We gave a total of 96 presentations this year to a range of external stakeholder groups.

International

- We participated in the 39th International Conference of Data Protection and Privacy Commissioners (ICDPPC) in Hong Kong. The Privacy Commissioner completed a three-year term as Chair of the ICDPPC.
- The Commissioner attended a Council of Europe plenary meeting about Convention 108 – the only international treaty on data protection.
- We attended two Asia Pacific Privacy Authorities (APPA) forums; the 48th forum in Vancouver and the 49th forum in San Francisco.

Enquiries and education

- We answered 9,147 enquiries; well over our expectation of 7,500.
- People made a total of 17,162 searches through our online FAQ tool, AskUs.
- We introduced a call centre service, live chat, and other changes to improve our enquiries function.
- We responded to 345 media enquiries.
- We launched our Privacy Trust Mark in May to recognise excellence in privacy-friendly products or services.

Breach notifications

- Agencies reported 168 breaches to the security of personal information this year.
- The Privacy Bill is set to make it mandatory for agencies to notify us of significant privacy breaches.

Information matching

- The Privacy Commissioner reviewed seven information matching provisions this year.
- The Commissioner recommended that section 295 of the Immigration Act 2009 should be repealed unless the Ministry of Justice can develop a more efficient process.
- There are 46 information matching programmes in operation.
- Seven programmes were not active this year.
- Five programmes transferred to operating under Approved Information Sharing Agreements.
- Parliament passed no new information matching provisions during the year. No new programmes began operating during the year.

9,147

enquiries

ESTIMATE:
7,500

4,845

completions of online modules

ESTIMATE:
2,500

345

media enquiries received

ESTIMATE:
200

50%

investigations resolved by settlement

ESTIMATE:
40%

15,000+

questions through AskUs

2

Privacy Trust Mark Awards

PRIVACY TRUST MARK
NOHO MATATAPU

Working towards our strategic goals

Our overall vision is to make privacy easy for New Zealanders. By promoting the Privacy Act as an enabling piece of legislation we hope that citizens, consumers, businesses, and government organisations will gain the benefits of safe and responsible personal information practices.

In our Statement of Intent 2017-2021, we set out three outcomes that we are working towards to support our vision. Our activities throughout the year have advanced our progress towards realising these outcomes by 2021.

Outcome 1
Increased citizen and consumer trust in the digital economy

Businesses and government organisations are reaping benefits from people's personal information, and new technologies are making that information more valuable and easier to access.

But New Zealand will not see these benefits if citizens and consumers do not trust agencies with their personal information. By providing effective regulation and promoting good privacy practices, we play a key role in building that trust.

Progress made

The results of our UMR survey showed that 62 percent of New Zealanders said they trust government organisations with their personal information, while 32 percent said they trust companies.

Our Investigations and Dispute Resolution team has continued to provide an independent and effective dispute resolution service for individuals with privacy complaints.

We made changes to our enquiries service and took lessons from our operational work to inform the public of their privacy rights and showcase good privacy practice to agencies.

The public has continued to use AskUs, our online FAQ, to answer their questions about privacy.

Look for activities marked with this icon to find out what else we have been doing to fulfil this outcome

Outcome 2
Innovation is promoted and supported

Privacy is not a barrier to technological advancement. We want to work across the public and private sectors to encourage innovation while keeping personal information safe and benefitting the public.

Progress made

We worked with the Government Chief Data Steward to develop principles for safe and effective data analytics. With data analytics and algorithms becoming more valuable to agencies, these principles should guide agencies towards safer and more secure data use.

We launched a Privacy Trust Mark scheme to recognise excellence in privacy-friendly products or services. We hope that this will encourage agencies to keep privacy in mind as they innovate and advance their practices.

With mandatory data breach notifications on the horizon for New Zealand, we have been working with the Office of the Australian Information Commissioner to learn from how they implemented a similar regime.

Look for activities marked with this icon to find out what else we have been doing to fulfil this outcome

Outcome 3
Increased influence to improve personal information practices

Building relationships with agencies is the most effective way we can help improve their personal information practices.

Progress made

We have worked on the Privacy Bill to strengthen privacy protection for individuals and help ensure that agencies comply with the law and good personal information practices.

We gave 96 presentations at regional centres around the country. We talked to agencies about current privacy issues, gave them the opportunity to engage in discussion, and promoted our online training and resources.

We collaborated with agencies such as the Privacy Foundation, Auckland Council, International Association of Privacy Professionals, Government Chief Data Steward, Domain Name Commission, New Zealand Police, Civil Aviation Authority, and Neighbourhood Support to put on events and produce resources that promote privacy compliance.

We also participated in privacy networks around the world to share knowledge and better prepare ourselves to address international privacy issues.

Look for activities marked with this icon to find out what else we have been doing to fulfil this outcome

Report on activities

Law reform

In addition to our regular duties, we have spent much of the year developing the Privacy Bill that will update and modernise New Zealand's privacy legislation.

From July to December 2017 we met regularly with Ministry of Justice officials to discuss and advise on various aspects of the Bill.

In January 2018, the Privacy Commissioner provided Minister of Justice Andrew Little with independent advice on the Bill's progress. The Commissioner recommended that officials prepare the Bill for introduction as a matter of priority, without deferring introduction for an Exposure Draft.

We continued to meet regularly with Ministry of Justice officials to support drafting of the Privacy Bill. They provided advice on:

- implementing the Law Commission's recommendations
- additional matters raised in the section 26 report
- drafting to ensure that the current provisions of the Privacy Act are carried over correctly into the new Bill.

In March 2018 we were consulted on and commented on the Cabinet Business Committee paper, and we provided independent advice on the Bill's readiness for introduction.

The Privacy Bill was introduced to Parliament on 27 March 2018. We subsequently provided detailed comment on the Introduction version and outstanding drafting matters.

In our submission, we urged the Select Committee to consider new policy initiatives that will make sure New Zealand's privacy framework is robust, fit-for-purpose and comparable to those of our trading partners. We also continued to work with Ministry officials to discuss outstanding issues in the Bill, including cross-border privacy rules.

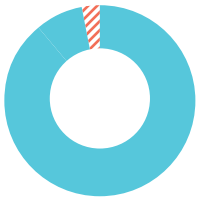
27 MAR

The Privacy Bill was introduced to Parliament

Dispute resolution

We closed 706 investigation files this reporting year. At the end of the reporting year, 89.1% of open investigation files were less than six months old. This is within 0.9% of our KPI.

We continue to have regular external reviews of our investigations. An independent reviewer assesses a selection of our investigations and scores out of 5 against a variety of criteria. This year the reviewer gave 95% of investigations assessed a score of 3.5 or higher.



95%

of investigations assessed by an independent reviewer received a score of 3.5 or higher

Figure 1
Age of open complaint files as at 30 June 2018

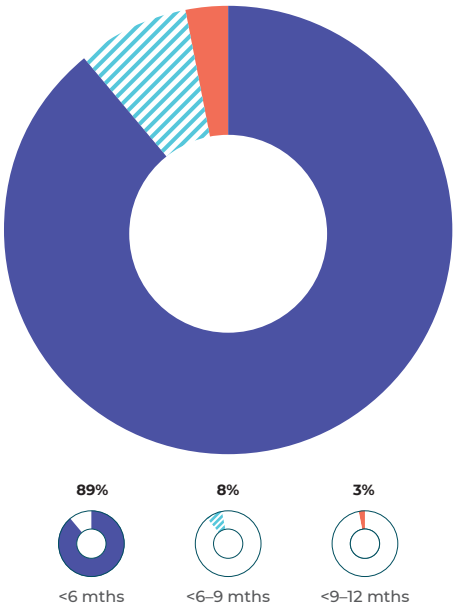
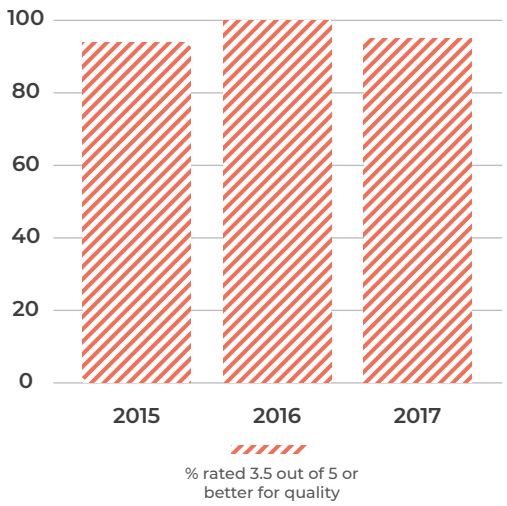


Figure 2
Result of complaint file reviews



Case Examples

CASE ONE

Woman denied copy of personal grievance case

A senior figure at an independent Crown entity was advised that an employee had raised a personal grievance case against her. She requested a copy of the personal grievance, which the Crown entity refused to provide, relying on section 29(1)(a) of the Privacy Act. This allows an agency to refuse to disclose information that would involve the unwarranted disclosure of the affairs of another person. The woman complained to our Office.

In this case the Crown entity had to balance the woman's right to access against the privacy interests of the person who made the personal grievance. The entity had consulted with the person who raised the grievance, and they did not support the disclosure. The entity also provided the woman with summaries that allowed her to understand the details of the grievance without disclosing extraneous material about the person who made it.

We found that the Crown entity appropriately balanced the competing rights in the case and correctly applied section 29(1)(a).

CASE THREE

Doctor discloses health information to employer

A heavy vehicle driver visited a doctor for an occupational health assessment. The doctor was acting as a contractor for the driver's employer. The doctor found that the driver had an eye condition that prevented him from driving, and subsequently provided health information to his employer and the New Zealand Transport Agency (NZTA).

The driver claimed that he did not authorise these disclosures and they contained inaccurate information. He made a complaint to our Office.

We were satisfied that the doctor was acting as the employer's medical officer to assess the driver's fitness to work, and had taken appropriate steps to make sure the assessment was accurate. The driver later acknowledged that he signed a medical certificate to give to his employer, and discussed disclosing the information to the employer and NZTA.

We formed the final view that the doctor had not interfered with the driver's privacy.

CASE TWO

Government employee snoops on neighbour

An employee at a government agency was in a personal dispute with his neighbour. The employee accessed the agency's files relating to the neighbour 73 times over three years. He also modified the man's file to add allegations of improper conduct. When the man found out, he made a complaint to our Office.

Under principle five of the Privacy Act, agencies must have safeguards in place to prevent the loss, misuse or disclosure of personal information. This does not require security processes to be foolproof; however we found that in this case the agency could have taken further steps to protect the man's information.

The employee had access to sensitive information, including his neighbour's information, in order to perform his duties. However, we were not satisfied that the agency trained the employee sufficiently about the seriousness and consequences of employee browsing. There was also no evidence that the employee was aware that his access may be randomly audited. This indicates that the employee either did not understand his obligations, or was confident he could browse without being caught.

We were satisfied that the neighbour suffered significant feelings of violation and humiliation in the circumstances. This enabled us to form the view that the agency had interfered with the neighbour's privacy.

The agency reviewed its processes but was unwilling to apologise to the neighbour or pay him financial compensation. We closed the file and gave the neighbour a certificate of investigation, which he could use to take his case to the Human Rights Review Tribunal.

CASE FOUR

Church shares details of marriage counselling with congregation

A Church made a statement to its members about a man's relationship with his wife, and the role the Church was playing in counselling them both. The man also had concerns that the Church made further disclosures, which included contact with another Church. He made a complaint to our Office.

The Church explained that it was a familial organisation, and that some members were already aware of the man's marriage difficulties. However, neither of these reasons fitted within the exceptions to principle 11 of the Privacy Act.

The man was clear about the emotional impact this disclosure had on him, including how it had preventing him from attending his son's engagement party. We were satisfied that the Church had interfered with the man's privacy by breaching principle 11 and causing him harm.

The Church offered to make a new statement to its membership addressing the issue, but the parties could not agree on the content. We closed the file and gave the man a certificate of investigation, which he could use to take his case to the Human Rights Review Tribunal.

CASE FIVE

Staff told of employee sacked for drug use

A woman was dismissed by her employer after drugs and drug-taking tools were seen in her car while it was parked in the company carpark. Three days after her dismissal, her manager emailed all employees disclosing the circumstances of her dismissal. The woman found out about the email and complained to our Office.

Under the Privacy Act, agencies should not disclose personal information for purposes other than those for which the information was obtained. The company accepted that personal information was disclosed, but claimed there was no breach because many staff already knew the information through workplace gossip.

We found that, while there was gossip in the workplace about the woman, the email from a senior manager carried considerably more weight and had contributed to the woman's significant humiliation, loss of dignity and injury to her feelings.

After we informed both parties of our view, they decided to resolve the matter themselves and later reached a settlement.

CASE SIX

Company shares customer phone numbers with marketers

A man complained to us about a payment management company that collected his personal information when he purchased one of its products. The company then passed the man's phone number on to a number of other agencies, which led to the man getting a number of unsolicited marketing calls.

We did not formally investigate the complaint because there was no indication of harm to the man. However we did take the opportunity to remind the company of its Privacy Act obligations and refer it to our online learning resources.

The company had a loosely worded and very permissive privacy statement. We encouraged it to use our 'Priv-o-matic' privacy statement generator to create a clear and compliant statement. We also recommended that the company reflect on the purpose for which it collects personal information and how it subsequently uses that information.

CASE SEVEN

Passenger makes vexatious requests to airline

A passenger contacted an airline, requesting all the information they had about him relating to a ticket dispute. When the airline delayed in responding to his requests, the man continued to call the airline for several months, requesting recordings of calls as he did so. The airline refused most of these additional requests, so the man complained to our Office.

Under the Privacy Act, an individual can request any personal information an agency holds about them, which can include recordings of calls. However an agency can refuse requests if they are vexatious.

This provision is rarely used, and there is a high bar for what can be considered vexatious. However in this case the man stated that he wanted to edit recordings and spread them through mainstream and social media to make the airline look "as bad as possible". We saw this as a clear intent to use the requests to aggravate and upset the airline and its staff.

Based on this, we found that these additional requests were vexatious and the airline could refuse them.

Figure 3
Top complaints by agency

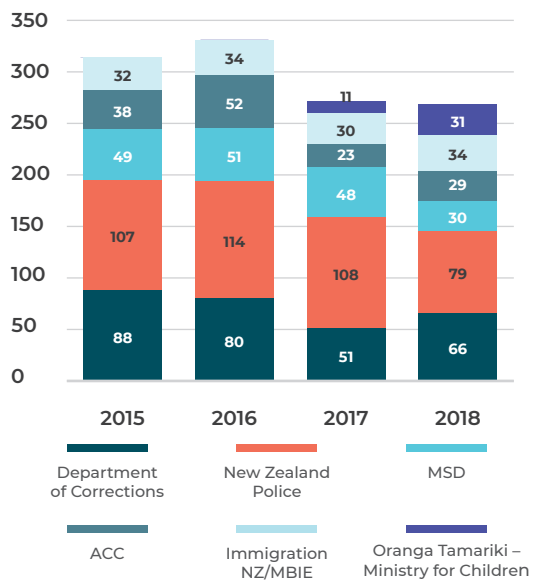


Figure 5
Settlement outcomes

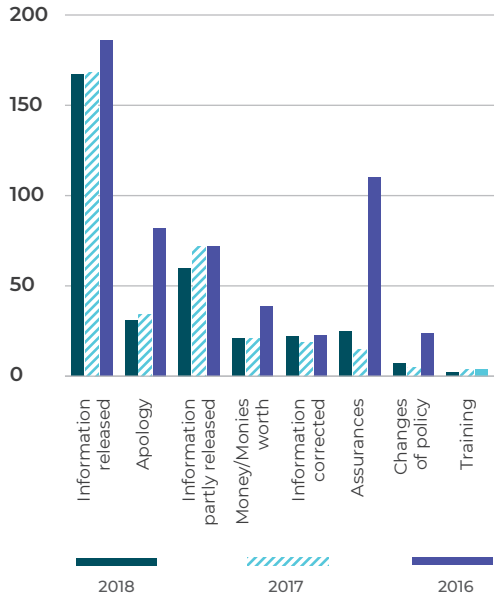
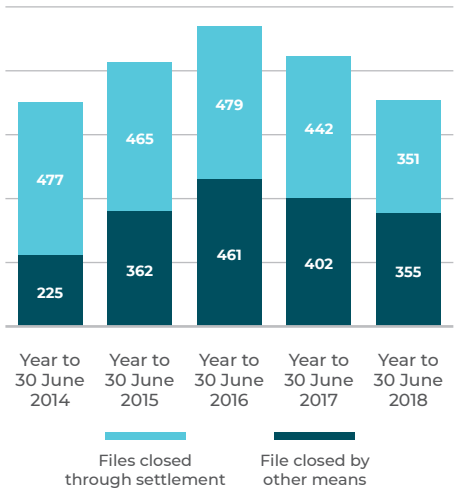


Figure 4
Files closed through settlement



Human Rights Review Tribunal

We aim to resolve most complaints during the course of the investigation. When the parties cannot reach an agreement, we can refer the matter to the Director of Human Rights Proceedings. The Director may choose to take the case to the Human Rights Review Tribunal. Complainants also have the right to take their case to the Tribunal themselves.

Cases introduced to the Tribunal

This year we referred five cases to the Director (a slight increase on last year). The Director has filed proceedings in one of those cases, and another has since been settled.

Twenty-nine complainants took proceedings to the Tribunal themselves, without a referral from us. This is a decrease from 37 in the previous year.

Tribunal delays

Significant delays in the Tribunal continued during this year. This has attracted significant media comment. Many Privacy Act cases that the Tribunal heard some time ago still await decisions, including one that the Tribunal heard in February 2015.

The Government has introduced an amendment to the Human Rights Act to address the delays. The amendment will allow the appointment of deputy chairpersons to share the chairperson's workload.

Tribunal decisions

We follow Tribunal decisions with interest because they provide us with guidance in interpreting the law and forming views when investigating Privacy Act complaints.

The Tribunal made decisions on nine Privacy Act cases this year. Six of those were dismissals, with no interference with privacy found. Of the three decisions that found an interference with privacy, two awarded damages to the plaintiffs.

A further nine cases filed in the Tribunal were withdrawn before they went to hearing.

Naming

Publicly naming organisations is one of the tools we use to incentivise 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 Facebook after it refused to cooperate with our investigation into a privacy complaint.

The social media company said the New Zealand Privacy Act did not apply to it and it did not have to comply with the Commissioner's request to review the information requested by the complainant.

While our investigations are almost always confidential, publicly identifying Facebook was necessary to highlight its demonstrated unwillingness to comply with the law, and to inform the New Zealand public of Facebook's position.

5

cases referred to the Director of Human Rights Proceedings

Codes of practice

At the start of the year there were six codes of practice in force.

Amending three codes

Just before the start of the year, we notified the public of our proposals to amend the Health Information Privacy Code, the Telecommunications Information Privacy Code, and the Credit Reporting Privacy Code. We proposed these amendments in response to amendments that the Intelligence and Security Act 2017 made to the Privacy Act. The aim was to keep a degree of consistency between Act and codes, except where differences are warranted.

After a public submission process, we made the amendments, and they came into effect at the same time as the amendments to the Privacy Act.

Review of credit reporting completed

This year we completed a public review of the comprehensive credit reporting system regulated by the Credit Reporting Privacy Code that we initiated in September 2016. We released two reports in May and June 2018 containing 32 formal findings and 19 recommendations for action.

Following the end of the reporting period in July we notified the public of a proposed amendment to the Code to give effect to 14 of the recommendations.

2

reports released in 2018 containing 32 formal findings and 19 recommendations for action

Policy

We work with agencies and ministries to help ensure that their policies treat personal information responsibly. This includes helping to develop policies, providing input on Cabinet papers, and submitting on legislation.

This year we advised on 107 policy proposals, mostly from government agencies, that involved personal information. We also published 14 submissions and formal reports.

We continue to have regular external audits of our policy work. An independent reviewer assesses a selection of our policy, information sharing, and information matching files and scores out of 5 against a variety of criteria. This year the reviewer gave close to 85% of policy files and 100% of information sharing and matching files assessed a score of 3.5 or higher.

Principles for the Safe and Effective use of Data and Analytics

Most of our policy work is demand-driven; agencies approach us for advice and guidance on how to handle personal information. When we have capacity for proactive work, we look for opportunities to consider emerging privacy issues.

An issue we focused on this year was agencies making decisions based on data analytics and algorithms.

In April 2018, the media reported that Immigration New Zealand (INZ) had been modelling the personal information of overstayers to identify which groups most commonly run up hospital costs or commit crime. This raised widespread concern from the public about the risk of racial profiling.

INZ put the programme on hold and consulted with us. Although we did not find evidence of racial profiling or any other cause for concern, the strong reaction to the story showed how heavily concerns about data analytics weighed on the public.

This is one of the reasons we collaborated with the Government Chief Data Steward to develop principles for safe and effective data analytics. These principles are intended to support the development of guidance for government agencies on using data and analytics for decision-making.

The principles are that an algorithm or risk modelling tool should:

- deliver clear public benefit
- ensure data is fit for purpose
- focus on people
- maintain transparency
- understand the limitations
- retain human oversight.

Submissions on Bills

By the time a Bill is introduced to Parliament, we usually will have had several opportunities to provide comments to help effectively address any privacy concerns.

If we have any outstanding concerns, we make a public submission on the Bill to make sure that Parliament has all the information it needs to make a decision

Overseas Investment Amendment Bill

The Overseas Investment Amendment Bill implements the Government's policy of banning purchases of residential land by overseas persons.

We submitted to the Select Committee that this Bill provided the Overseas Investment Office (OIO) with unnecessarily broad information gathering powers. These powers create the potential for the OIO to make overly intrusive requests about individuals that it has no reason to believe are ineligible to purchase sensitive residential land.

The Select Committee agreed with some of our recommendations and improvements were made as a result.

End of Life Choice Bill

The End of Life Choice Bill provides people who have a terminal illness or a grievous and irremediable medical condition with the option to request assistance from a medical practitioner to end their life.

We made a number of recommendations to clarify how individuals' health information would be treated under the Bill. Because this Bill is of high public interest and may change significantly, we offered our assistance to the Ministry of Health to make sure that the Bill provides appropriate protection of, and access to, personal information.

The Select Committee has not yet reported back at the time of writing.

Employment Relations Amendment Bill

The Employment Relations Amendment Bill implements the Government's commitments in employment relations by changing minimum standards and protections to strengthen collective bargaining and union rights in the workplace.

Our select committee submission focused on how the Bill requires employers to share certain information about new employees with unions, unless the employee objects. We considered this to be poor privacy practice, and against an individual's right to exercise some autonomy over their personal information.

Our recommendations were not implemented.

Other matters

Law Commission review of Abortion Law Reform

The Government has asked the Law Commission to provide advice on alternative approaches for abortion legal frameworks to align with a health approach.

We support the goal of ensuring that New Zealand law treats abortion as a health issue. Handling abortion solely as a health matter will better ensure that the decision to abort is treated consistently with the fundamental privacy in bodily self-determination. It will also ensure abortion is governed consistently by the law governing the privacy of health information.

Police Vetting Service

In October 2016, we released a joint review with the Independent Police Conduct Authority (IPCA) of the Police Vetting Service. The Government has progressed a key recommendation of the joint review by publicly consulting on establishing a clear statutory framework for the Police Vetting Service. We are pleased with this development, and have made a joint submission with IPCA to the New Zealand Police.

Royal Commission of Inquiry into Historical Abuse in State Care

The Government has launched the Royal Commission of Inquiry into Historical Abuse in State Care.

We submitted on the draft Terms of Reference for the Royal Commission, providing observations of how relevant agencies handle individuals' requests for personal information under the Privacy Act. We also made recommendations on how the Royal Commission could gather and make available information about individuals.

Outreach

While online tools are very useful, there is still significant value in engaging with the public in person. To that end, we gave a total of 96 presentations to a range of audiences during the year.

We also promoted privacy and data protection during Privacy Week, and learned more about the public's attitude towards privacy with our latest UMR survey.

Regional visits

The Privacy Commissioner regularly visits areas outside the main centres to strengthen our connections and promote our resources.

During these visits, the Commissioner holds public meetings and presents to DHBs, local government, NGOs, and other groups. The Commissioner speaks about the latest developments in privacy rights and protections, and takes questions from the audience.

In the reporting period, the Commissioner visited:

- Horowhenua and Levin (August 2017)
- Napier and Hastings (September 2017)
- Masterton (October 2017)
- Hamilton and Tokoroa (March 2018)
- Christchurch (April 2018).

Bill briefings

We gave a concentrated round of briefings to stakeholder groups on the Privacy Bill. We partnered with law firms and consultancies to brief clients on the Bill at lunchtime and after work sessions. Over eight weeks we reached over 1,000 representatives of the business sector in Auckland and Wellington.

96

presentations given to a range of audiences during the year

PrivacyLive

Our PrivacyLive speaker series continued throughout the reporting period. At the beginning of 2018 we began holding events in Auckland in collaboration with the Privacy Foundation, Auckland Council and the International Association of Privacy Professionals.

We held eight PrivacyLive events in Auckland and Wellington with a range of speakers:

- KPMG and OPC Panel on information sharing – 2 November 2017 (Wellington)
- PrivacyLive forum on Encryption – 7 December 2017 (Wellington)
- Blockchain's promise for privacy – 27 February 2018 (Auckland)
- Machine Learning, Big Data and Being Less Wrong – 13 March 2018 (Wellington)
- Orwell's 1984 panel discussion – 14 March 2018 (Auckland)
- CERT NZ update and incident report – 19 March 2018 (Wellington)
- Working Towards Trusted Data Use – 11 April 2018 (Auckland)
- Privacy Unplugged with the Privacy Commissioner – 7 May 2018 (Auckland).

We livestreamed these events online so people who could not make it in person could watch.

Right to Know Day

We marked "Right to Know" Day in partnership with the Office of the Ombudsman in late September 2017, and ran a joint discussion panel event that was recorded by Radio New Zealand.

Privacy Week

Privacy Week is an annual event across the Asia-Pacific, organised by the Asia Pacific Privacy Authorities (APPA). It is an opportunity to raise awareness of privacy and data protection through a week of activity across the region.

Our Privacy Forum at Te Papa Tongarewa was the highlight of Privacy Week 2018. It attracted over 300 representatives from the public and private sectors, and wider civil society. Minister of Justice Andrew Little gave the opening address and the forum featured a variety of speakers discussing automated decision making, GDPR, and New Zealand's privacy law reform. We received very positive feedback on the event.

During the week we also released and promoted a number of resources:

- An animated video and printable infographic promoting everyday privacy rights and responsibilities
- The results of our latest UMR survey of public attitudes to privacy
- Joint guidance with the Domain Name Commission on being privacy conscious with domain name registrations
- A Privacy Week quiz

UMR privacy survey

Every two years we commission UMR Research to carry out a survey of the New Zealand public's attitudes towards privacy.

This year's results showed that:

- more than half (55 percent) of all New Zealanders are more concerned with their individual privacy now than they were in the last few years
- the number of people concerned about their individual privacy has risen by two percent (to 67 percent) since the last survey held in 2016
- those with a household income of $50,000 or less are more likely to be concerned about individual privacy (77 percent) compared to those with a higher household income (63 percent)
- the privacy issue New Zealanders are most concerned about is children putting information about themselves on the internet
- sixty-two percent of New Zealanders trust government organisations with their personal information, a drop of nine percent from when this was last measured in 2014
- thirty-two percent of New Zealanders trust companies with their personal information
- respondents felt vulnerable when sharing personal information over social media.

67%

of people are concerned about their individual privacy, an increase of two percent

International

We participated in several international forums this year, principally:

- the International Conference of Data Protection and Privacy Commissioners (ICDPPC)
- a plenary meeting of the Council of Europe's international data protection treaty, Convention 108
- two Asia Pacific Privacy Authorities (APPA) meetings.

International Conference of Data Protection and Privacy Commissioners

At the 39th annual Conference in Hong Kong the Privacy Commissioner completed a three-year term as Chair of the Conference. Our Office also completed three years of providing a Conference Secretariat. In these roles we took the opportunity to substantially contribute to advancing capacity building and strategic work among privacy authorities at an international level.

Some significant achievements this year included:

- running the first global census of privacy regulators
- delivering a series of regional enforcement cooperation workshops
- hosting an awards programme for privacy authorities to showcase innovation
- arranging a full day in-depth discussion between the world's privacy commissioners about government information sharing.

Plenary Meeting of the Committee of Convention 108

The Council of Europe is home to the only international treaty on data protection, the "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data", known as Convention 108.

New Zealand gained "observer" status in 2017, and in June 2018 the Privacy Commissioner attended the 36th Plenary Meeting of the Committee of Convention 108 in Strasbourg, France to investigate whether he should recommend that the New Zealand Government apply to accede to the convention.

This year the Convention has been modernised and updated, and the new convention (108+) will soon be open for signature. Representatives from Africa, Asia and South America were present to find out about the effects of 108+.

The Commissioner found that Convention 108+ has potential to fill some gaps in international law and set a new international standard. The current state of New Zealand law is likely to make it difficult to take on the legal obligations of 108+, but the Privacy Bill presents an opportunity to bring our law closer to what may well emerge as a benchmark.

Asia Pacific Privacy Authorities Forum

The Asia Pacific Privacy Authorities Forum brings together 19 privacy enforcement authorities from across the Pacific. At the meetings authorities work to foster cooperation and information sharing and continuously improve regulatory performance.

In November 2017 we attended the 48th meeting in Vancouver, Canada, with a special emphasis on partnering for privacy research. In June 2018 we attended the 49th meeting in San Francisco, USA, focussing on technology issues relating to privacy.

Enquiries and education

This year our AskUs tool gave us the capability to start a call centre service to resolve basic enquiries. We also began operating a new live chat function on our website, giving the public another way to engage with us.

We made these changes to ensure that we are providing a flexible, accessible, and useful enquiries service that meets the needs of the public.

This year we answered 9,147 enquiries, well over our estimate of 7,500. Of these, we responded to 5,453 enquiries in-house and the call centre responded to the other 3,694.

AskUs

In the reporting year we received a total of 17,162 searches through our online FAQ tool AskUs. This is a significant increase over the last reporting year, when we received 8,433.

This year's results include searches by both call centre and Office staff, who use AskUs to answer enquiries. Using AskUs has helped us become more efficient in responding to enquiries and improved quality control.

We received a high number of searches in May 2018. This coincided with media and public interest in CCTV cameras using facial recognition technology, and with Privacy Week. We saw an increase in the use of search terms "facial recognition", "biometric", and "CCTV".

We are continuously refining existing content based on user feedback.

Call centre

Our Enquiries Officers each typically dealt with an average of nine enquiries files a day, with the large majority coming in by phone. Many of these enquiry calls were about simple issues with straightforward answers. Some were mistakenly made to the wrong agency.

On 1 November 2017 we started a three month trial of a call centre service with the aim of reducing the number of calls coming through to our Office.

The trial showed that the call centre was effective in catching enquiries that were easy to resolve. Call centre staff were able to transfer calls to the correct agency, and use AskUs to resolve basic enquiries.

By the end of the trial period, the number of calls being forwarded to our Office dropped significantly. The call centre had taken around 90% of the telephone enquiries, only referring on calls that were too complex or needed escalation.

This gave Enquiries Officers more time to devote to the complex enquiries that had been referred to them, allowing them to provide more thorough and satisfying resolutions to the enquirers. It also alleviated the stress on office staff from the repetitious nature of some calls.

Based on these results, we continued with the call centre service. It remains effective in supporting enquirers and directing them to the tools available to assist them online. Filtering out the repetitive enquiries has also allowed us to develop our in-house expertise.

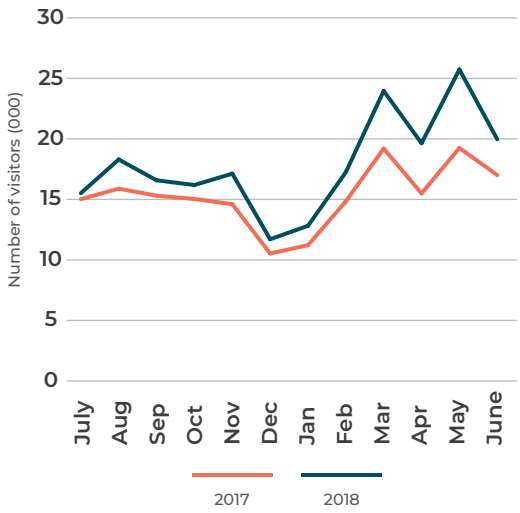
Live chat

In response to increasing demand for online solutions, we created a live chat tool for our website. Our aim was to give users another way to engage with our staff and ask questions about the Privacy Act.

After running a trial in mid-2017, we launched the tool in June 2018. Our newly established Assistant Investigator roles brought the capacity and technical knowledge to operate live chat effectively.

We plan to monitor this tool's effectiveness, and expand its availability and functions as appropriate.

Figure 6
Unique website visitors

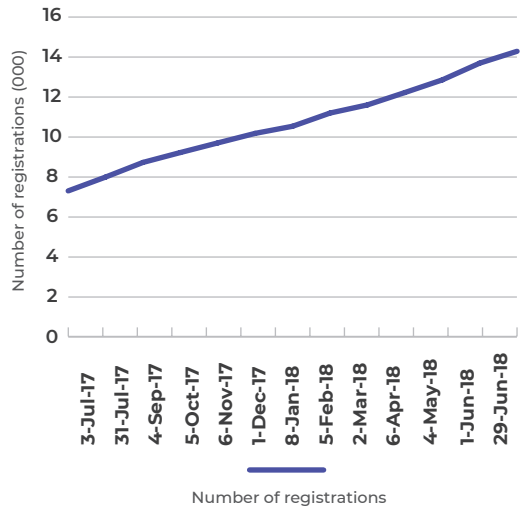


Online modules

Our free online education modules continue to demonstrate consistent growth in uptake. Notable is the significant number of registrants for "Privacy ABC" – our 30 minute introductory module, which we launched in June 2017. More than 3,000 people had registered by the end of the reporting period.

We now offer eight education modules covering a range of topics. Our newest module is "Health ABC", our introduction to protecting health information. We developed this module throughout the year and launched it after the end of the reporting period.

Figure 7
Cumulative online training module registrations



Privacy Trust Mark

At the Privacy Forum in May 2018 we launched the Privacy Trust Mark scheme to recognise excellence in privacy-friendly products and services. The Trust Mark aims to give New Zealanders confidence that a product or service has been designed with their privacy interests in mind.

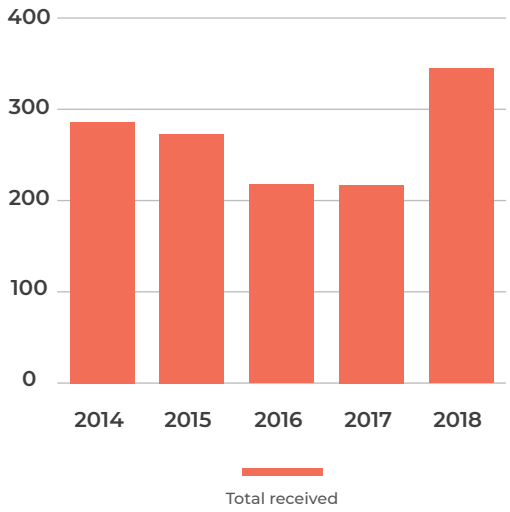
We awarded the first Privacy Trust Marks to Trade Me's 'Transparency Reporting' and the Department of Internal Affairs' RealMe identity verification service. We received two more applications for the Trust Mark before the end of the reporting year.

Media

There was a particularly high level of media activity in 2017/18 with 345 media enquiries received (up 59% from 2016/17 activity and comparable activity in 2015/16).

A number of high-profile issues drove this increased interest, including the revelations about Facebook and Cambridge Analytica, the effect of the GDPR, the Privacy Bill, and several significant data breaches.

Figure 8
Media enquiries received



Guidance on security cameras and drones

We prepared a user-friendly guidance card on security cameras and drones and distributed it to electronic goods retailers before Christmas 2017. We created the card in partnership with the Civil Aviation Authority, Neighbourhood Support, and New Zealand Police. It provides tips on how to use security cameras and drones without infringing on the privacy rights of others.

Breach notifications

We receive voluntary breach notifications from a variety of public and private sector agencies. We encourage this because we can guide agencies on how they should respond to breaches, and how they can stop them from happening again.

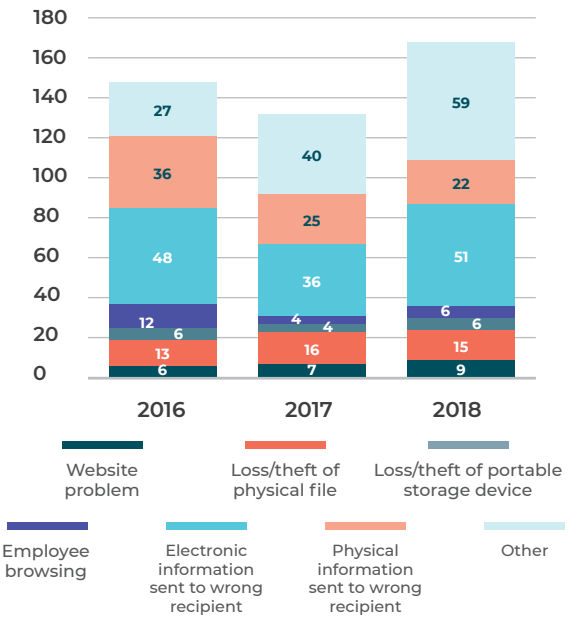
Breaches that agencies report can help us identify common privacy issues and risks. We also use the lessons learned from these breaches to educate agencies about good information handling practices.

This year agencies reported 168 breaches to us. Ninety-one of those notifications were from public agencies and the other 77 were from private agencies.

Because breach reporting is voluntary, there is no way of knowing what proportion of all the breaches that occur are reported to our office.

Human error, e.g. sending information to the wrong person, continues to cause most of the breaches that agencies report to us.

Figure 9
Common types of breaches



Getting ready for mandatory breach notifications

The Privacy Bill before Parliament is set to make it mandatory for agencies to notify us of significant privacy breaches. We support this and see it as critical in making agencies more accountable for their handling of personal information.

In our submission on the Privacy Bill, we recommended that the threshold for notification should be clarified. We also recommended that the Bill include a duty to minimise harm and provide for follow-up reporting.

Australia's mandatory data breach notification legislation came into force in February 2018. We have been liaising closely with our Australian counterpart, the Office of the Australian Information Commissioner, to learn from the implementation of the new law in its jurisdiction.

168

breaches reported to us, 91 of those notifications were from public agencies and the other 77 were from private agencies

Information matching

Statutory review of information matching provisions

Section 106 of the Privacy Act requires us to review the operation of each information matching provision every five years. In these we recommend whether a provision should continue, be amended, or be cancelled.

This year we reviewed seven information matching provisions. We recommended that section 295 of the Immigration Act 2009 should be repealed unless the Ministry of Justice (MoJ) can develop a more efficient process.

The full review reports are available on our website: privacy.org.nz/info-matching-reports

Births, Deaths, Marriages, and Relationships Registration Act 1995, section 78A

This provision allows Immigration New Zealand (INZ) to receive death information from the Department of Internal Affairs (DIA) to update INZ's database of overstayers and temporary permit holders.

Citizenship Act 1977, section 26A

This provision allows INZ to receive citizenship information from the DIA to remove new citizens from INZ's database of overstayers.

Corrections Act 2004, section 181

This allows INZ to advise the Department of Corrections of prisoners who are subject to deportation.

Customs and Excise Act 1996, section 280

This provision allows the New Zealand Customs Service (Customs) to supply the MoJ with arrival and departure information of debtors with significant amounts outstanding.

Immigration Act 2009, section 295

This provision allows INZ to supply the MoJ with arrival and departure information to help locate people who owe fines.

This match is no longer effective and should be repealed unless the MoJ can develop a new business case.

Tax Administration Act 1994, section 85A

This provision allows Inland Revenue (IR) to supply the MoJ with contact information for people who owe fines.

Electronic Identity Verification Act 2012, section 39

This provision allows the DIA to verify identity information provided by an applicant in support of their application for an electronic identity credential and to keep that information current.

Changes in authorised and operating programmes

There are currently 46 information matching programmes in operation (see Appendix B). There are also seven programmes that were not active this year, and five programmes that transferred to operating under Approved Information Sharing Agreements.

New provisions and programmes

Parliament passed no new information matching provisions during the year. No new programmes began operating during the year.

Programmes suspended

The Ministry of Business, Innovation and Employment did not operate their programme with Customs to identify people who might qualify as motor vehicle traders (Motor Vehicle Sales Act 2003 s.120 and s.121).

The Ministry of Education did not operate their programme with the DIA for birth records. However, they are considering re-starting this programme (Births, Deaths, Marriages, and Relationships Registration Act 1995 s.120 and s.121).

The Ministry of Health (MoH) did not operate their programme with INZ to determine eligibility for access to publicly funded health and disability support services. This is because the MoH was continuing to process the results of previous matches (Immigration Act 2009, s.300).

The MoJ ceased to operate their programme with INZ for arrival and departure information to help locate people who owe fines. This is because of the significant manual effort involved and the comparatively low benefits from the programme. The MoJ is considering alternative approaches to receive the information (Immigration Act 2009, s.295).

The Ministry of Social Development (MSD) did not operate their Periods of Residence sampling match with Australia for superannuation entitlement. The MSD advises that Australia's concerns with Australian privacy law have been resolved and therefore they may resume operating the programme (Social Welfare (Reciprocity Agreements, and New Zealand Artificial Limb Service) Act 1990, s.19C and s.19D and Social Welfare (Reciprocity with Australia) Order 2002).

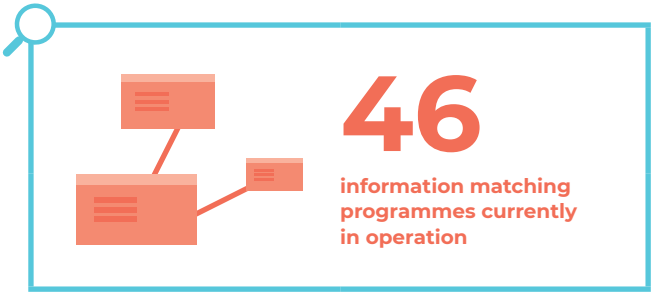
MSD also did not need to use the provision to allow IR to respond to tax information enquiries from the Netherlands social welfare authorities, as no requests were received from the Netherlands. (Social Welfare (Reciprocity Agreements, and New Zealand Artificial Limb Service) Act 1990, s.19C and s.19D and Social Welfare (Reciprocity with the Netherlands) Order 2003 and Tax Administration Act 1994 s.85B)

MSD did not use powers to require information for matching from employers under section 11A of the Social Security Act 1964.

Programmes ceasing:

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

- MSD/IR Family Assistance Administration
- MSD/IR Family Support Double Payment
- IR/MSD Commencement/Cessation – Benefits
- IR/MSD Commencement/Cessation – Students
- IR/MSD Community Services Card



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

We employ staff in our Auckland and Wellington offices.

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

The Assistant Commissioner (Policy & Operations) is responsible for investigations and dispute resolutions, enquiries, policy and technology advice, and information matching work.

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

The General Manager is responsible for administrative and managerial services. We employ administrative support staff in both offices.

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

The Office of the Privacy Commissioner promotes 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 integrated into the human resource programmes that are outlined in our Statement of Intent 2017-2021. The policy encourages active staff participation in all EEO matters. We review this policy annually, together with policies on recruitment, employee development, harassment prevention, and health and safety.

During the year, the main areas of focus continue to be:

- developing talent regardless of gender, ethnicity, age or other demographic factor
- integrating work practices which promote or enhance work life balance amongst employees, including family friendly practices
- maintaining equitable gender-neutral remuneration policies which are tested against best industry practice
- placing a strong emphasis on fostering a diverse workplace and inclusive culture.

We benefit from a diverse workforce from a variety of different ethnicities, including Māori, Asian, and other ethnic groups.

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.

Our 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.

We have an appointed harassment officer, and staff have ready access to external support through our employee assistance programme.

Workplace gender profile – as of 30 June 2018

Role	Women		Men		Total
	Full-time	Part-time	Full-time	Part-time	
Commissioner			1		1
Senior managers	2		2		4
Team and unit managers	2	1	1		4
Investigations and Dispute Resolution	5	1	4		10
Administrative support	6	1			7
Advisers (policy, commmunications and legal)	5		4		9
Total	**20**	**3**	**12**		**35**

Finance and performance report

Statement of responsibility

Under 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 2018.

J Edwards
Privacy Commissioner
29 October 2018

G F Bulog
General Manager
29 October 2018

Statement of performance

The Justice Sector has an aspirational outcome that all New Zealanders should expect to live in a safe and just society. We support this aspiration as a Justice Sector Crown entity.

While the Office of the Privacy Commissioner is an independent Crown entity and strongly maintains such independence, our Statement of Intent and Statement of Performance Expectations set out a work programme that complements this aspiration and government priorities as a whole.

Our Statement of Intent 2017-2021 identifies three high level outcomes to support our vision to make privacy easy. The "Working towards our strategic goals" section of this Annual Report has provided an overview of the work we have undertaken this reporting year to support our progress towards these outcomes.

The Statement of Performance Expectations for the year to June 2018 identified four output classes to support these three outcomes. These have remained consistent from previous years. We report our progress against these output areas in this section.

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	230	292
Total revenue	**5,200**	**5,262**

The operating grant is received as part of the Non-Departmental Output Expenses – Services from the Privacy Commissioner within Vote Justice. This appropriation is limited to the provision of services concerning privacy issues relating to the collection and disclosure of personal information and the privacy of individuals.

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 1.7% of the total Vote Justice Non-Departmental Output Expenses Appropriation for 2017/18. The total expenses in the year are $5,201k as set out in the cost of service statement below.

Cost of service statement

for the year ended 30 June 2018

As set out in the 2017/18 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:

	Actual 2018 $000	Budget 2018 $000	Actual 2017 $000
OUTPUT CLASS 1: GUIDANCE, EDUCATION AND AWARENESS			
Resources employed			
Revenue	839	785	742
Expenditure	721	694	635
Net Surplus/(Deficit)	**118**	**91**	**107**
OUTPUT CLASS 2: POLICY AND RESEARCH			
Resources employed			
Revenue	1,955	1,999	2,038
Expenditure	2,063	2,168	2,062
Net Surplus/(Deficit)	**(108)**	**(169)**	**(24)**
OUTPUT CLASS 3: INFORMATION SHARING/MATCHING			
Resources employed			
Revenue	789	683	775
Expenditure	704	590	680
Net Surplus/(Deficit)	**85**	**93**	**95**
OUTPUT CLASS 4: COMPLIANCE			
Resources employed			
Revenue	1,679	1,733	1,614
Expenditure	1,713	1,816	1,716
Net Surplus/(Deficit)	**(34)**	**(83)**	**(102)**
TOTALS			
Resources employed			
Revenue	5,262	5,200	5,169
Expenditure	5,201	5,268	5,093
Net Surplus/(Deficit)	**61**	**(68)**	**76**

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 Non-Departmental Output Expenses – Services from the Privacy Commissioner 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 this is important

One of our functions 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. Over the period covered by the Statement of Intent, there will be a specific focus on reaching out to diverse communities. We also produce a range of guidance and other resource material.

During the reporting year, we increasingly used our website to provide these services online, particularly through online modules and the AskUs tool.

Output Measures

Measure	Estimate	Achieved 2017/18	Achieved 2016/17
Quantity			
Number of people completing education modules on the online system.	2,500	**Achieved** 4,845 people have completed e-learning modules in the year to 30 June 2018. 2,286 of these relate to completions of post course quizzes for Privacy 101, Health 101, PIA and CRPC. A further 2,559 relate to completions of the final unit of the Privacy ABC module which went live towards the end of June 2017.	Achieved – 2,761
Presentations at conferences and seminars.	90	**Achieved – 96**	Achieved – 107
Public enquiries received and answered.	7,500	**Achieved – 9,147**	Substantially achieved – 7,320
Media enquiries received and answered.	200	**Achieved – 345**	Not achieved – 217
Blog posts and case notes created.	90	**Not achieved – 60** 50 blog posts and 10 case notes.	n/a – new measure

Measure	Estimate	Achieved 2017/18	Achieved 2016/17
Quality			
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 – 94%**[1]	Achieved – 98%
Timeliness			
Respond to all enquiries within two working days.	100%[2]	**Substantially achieved – 95%**	93% responded to within one working day
Guidance materials are produced within agreed timelines as set out in the work plan.	Achieved	**Achieved**	Achieved

1 The satisfaction rate is measured as a simple ratio of the fifth question in the Office's annual external stakeholder survey run through SurveyMonkey. There were 63 responses to this question. SurveyMonkey has some limitations. Records can be deleted and modified, and the reported result may not be completely free from error.

2 This target was included within the Non-Departmental Output Expenses – Services from the Privacy Commissioner appropriation and was the same as the SPE target.

Output class 2: Policy and research

Why this is important

We actively comment on legislative, policy or administrative proposals that affect privacy to make sure the proposals take the Privacy Act's requirements into account. We are also actively involved in international meetings. This gives us the ability to identify and respond to emerging issues in a timely manner.

Output Measures

Measure	Estimate	Achieved 2017/18	Achieved 2016/17
Quantity			
The number of the following pieces of work completed during the year:			Achieved
• Proposals involving the use of personal information or other privacy issues, received for consultation or advice from the public and private sectors;	100	**Achieved – 107**	186
• Submissions and other formal reports, including submissions to select committees; and	15	**Not achieved – 14**	22
• Office projects, including research projects.	10	**Achieved – 11**	15
Identifiable progress in international efforts in which we are actively engaged to work towards more sustainable platforms for cross border cooperation.	Achieved	**Achieved** The Office was represented at and contributed to a number of different regional and international meetings during the year – APPA, ABLI and ICDPPC. There has been ongoing work with OECD to develop internationally comparable breach notification metrics. The Office's three year term as the ICDPPC Chair Secretariat ended and an International Engagement Strategy was endorsed by the Office.	Achieved

Measure	Estimate	Achieved 2017/18	Achieved 2016/17
Quality			
The percentage of recipients of policy advice who are satisfied with the service they received from the Privacy Commissioner.	85%	**Achieved – 87%**[3]	Achieved – 93%
Our participation in the law reform process is valued by the Ministry of Justice.	Achieved	**Achieved** Based on feedback received directly from the Ministry of Justice.	Achieved
The percentage of externally reviewed policy files that are rated 3.5 out of 5 or better for quality.	85%	**Substantially achieved – 83%** Based on findings from an independent review of a sample of policy files closed in the year.	Substantially achieved – 80%
Timeliness			
The percentage of policy files where advice was delivered within agreed timeframes.	100%	**Substantially achieved – 97%**	Substantially achieved – 96%
Responses to requests for input into law reform are made available within agreed timelines.	100%	**Not achieved** Based on the annual stakeholder survey results, 93% of law reform related respondents noted that the timeframe had been met. Only one respondent indicated that the timeframe had not been met.[4] In addition, direct correspondence with the Ministry of Justice regarding the Office's input into the law reform process has been positive and no timeliness issues have been identified.	Achieved – 100%

3 The satisfaction rate is measured as a simple ratio of the first question in the Office's annual external stakeholder survey run through SurveyMonkey. There were 39 responses to this question relating to policy advice. SurveyMonkey has some limitations. Records can be deleted and modified, and the reported result may not be completely free from error.

4 The satisfaction rate is measured as a simple ratio of the second question in the Office's annual external stakeholder survey run through SurveyMonkey. There were 15 responses to this question relating to law reform. See footnote 3 above for limitations.

Output class 3: Information sharing and matching

Why this is important

We have 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). We also provide advice to agencies carrying out information sharing and matching about how to meet their responsibilities under Part 9A and Part 10 respectively.

Output Measures

Measure	Estimate	Achieved 2017/18	Achieved 2016/17
Quantity			
The number of information matching programmes monitored under Part 10 of the Privacy Act.	54	**Achieved – 58** (46 current programmes, seven inactive programmes and five that were replaced by AISAs in August 2017)	56
The number of new Approved Information Sharing Agreements received for consultation under s96O of the Privacy Act.	2	**Achieved – 4**	Achieved – 4
The number of formal reports produced that relate to information sharing or information matching programmes, under sections 96P, 96X, 96O or 106 of the Privacy Act.	8	**Achieved – 9**	Not achieved – 6
The number of proposals consulted on involving information sharing or matching between government agencies, completed during the year.	10	**Achieved – 38**	Achieved – 33

Measure	Estimate	Achieved 2017/18	Achieved 2016/17
Quality			
The percentage of recipients of information sharing and matching advice that are satisfied with the service they received from the Privacy Commissioner.	85%	**Achieved – 90%**[5]	Achieved – 95%
The percentage of externally reviewed information sharing and matching files that are rated as 3.5 out of 5 or better for quality.	85%	**Achieved – 100%** Based on findings from an independent review of a sample of information sharing and matching files closed in the year.	Substantially achieved – 80%
The Trusted Sharing Consultancy Service is valued by those agencies that have engaged the Office in this capacity.	Achieved	**Achieved** As reported above, 90% of respondents to the annual stakeholder survey who dealt with the Office either through this service or in an information sharing capacity were satisfied with the service provided.[6] Note that this result is likely to include some respondents who may have dealt with the Office in relation to the reporting aspects of information sharing/matching, which would not be part of the consultancy service. It is not possible to quantify this. From 2019, only satisfaction with information sharing/matching advice as a whole will be reported as in previous years.	N/A – new measure
Timeliness			
The percentage of information sharing and matching files where advice was delivered within agreed timeframes.	100%	**Substantially achieved – 98%**	Substantially achieved – 98%

5 The satisfaction rate is measured as a simple ratio of the first question in the Office's annual external stakeholder survey run through SurveyMonkey. There were 30 responses to this question relating to information sharing/matching and the Trusted Sharing Consultancy Service. SurveyMonkey has some limitations. Records can be deleted and modified, and the reported result may not be completely free from error.

6 As per footnote 5 above.

Output Class 4: Compliance

Why this is important

Another of our core functions is the provision and management of an independent and responsive complaints and investigation process. We continue to transform the way we deal with complaints, with a focus on more timely resolutions. During the 2014/15 year we introduced an online complaints lodgement system. In this reporting year 45% of all complaints were lodged in this way.

We also review and amend codes of practice.

Output Measures

Measure	Estimate	Achieved 2017/18	Achieved 2016/17
Quantity			
Number of complaints received.	900	**Not achieved – 807**	736
Number of data breach notifications received.	100	**Achieved – 168**	132
Quality			
The percentage of complainants' and respondents' who rate their satisfaction with the complaints handling process as "satisfactory" or better.	60%[7]	**Not achieved – 35%** The % reported here only represents the views of a small number of complainants and no respondents. A review of the survey process was due to be undertaken in 2017/2018 but this was delayed. From 2018/19 this KPI has been removed so that the Office can reassess alternative mechanisms for measuring satisfaction.	Not achieved – 43%
The percentage of complaints files closed by settlement between the parties.	40%[8]	**Achieved – 50%**	Achieved – 48%
Amendments to Codes of Practice meet all statutory requirements.	100%	**Achieved** Amended 3 Codes of Practice in September 2017 to give effect to Intelligence and Security Act statutory amendments to the Privacy Act.	Achieved

Measure	Estimate	Achieved 2017/18	Achieved 2016/17
The percentage of externally reviewed complaints investigations that are rated as 3.5 out of 5 or better for quality.	85%	**Achieved – 95%** Based on the results of an external review of a sample of complaints files closed between July 2017 and June 2018.	Achieved – 100%
Timeliness			
The percentage of open files greater than 6 months old at the year end.	10%	**Not achieved – 11%**	Achieved – 10%
Review of the operation of Credit Reporting Code completed and actioned.	Achieved	**Achieved** The review was completed with formal reports released in May and June.	Achieved

7 This target was included within the Non-Departmental Output Expenses – Services from the Privacy Commissioner Appropriation and was the same as the SPE target.

8 As per footnote 7 above.

Statement of accounting policies

for the year ended 30 June 2018

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 New Zealand public, as opposed to that of making a financial return. Accordingly, the Privacy Commissioner has designated itself as a public benefit entity for financial reporting purposes.

The financial statements for the Privacy Commissioner are for the year ended 30 June 2018, and were approved by the Commissioner on 29 October 2018. 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.

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 from 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 are presented 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, IR – 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 2018:

- 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 2018

	Note	Actual 2018 $000	Budget 2018 $000	Actual 2017 $000
Revenue				
Crown revenue	2	4,970	4,970	4,970
Other revenue	2	292	230	199
Total Income		**5,262**	**5,200**	**5,169**
Expenditure				
Promotion	4	125	94	55
Audit fees		30	30	30
Depreciation and amortisation	4,9,10	194	223	185
Rental expense		417	421	411
Operating expenses		762	637	621
Contract services		177	83	84
Staff expenses	3	3,496	3,780	3,707
Total expenditure		**5,201**	**5,268**	**5,093**
Surplus/(Deficit)		**61**	**(68)**	**76**
Other comprehensive revenue and expenses		–	–	–
Total comprehensive revenue and expenses		**61**	**(68)**	**76**

Explanations of major variances are provided in Note 1.
The accompanying notes and accounting policies form part of these financial statements

Statement of changes in equity

for the year ended 30 June 2018

	Note	Actual 2018 $000	Budget 2018 $000	Actual 2017 $000
Total equity at the start of the year		1,119	1,119	1,043
Total comprehensive revenue and expenses for the year		61	(68)	76
Total equity at the end of the year	**5**	**1,180**	**1,051**	**1,119**

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

Statement of financial position

as at 30 June 2018

	Note	Actual 2018 $000	Budget 2018 $000	Actual 2017 $000
Public equity				
General funds	5	1,180	1,051	1,119
Total public equity		**1,180**	**1,051**	**1,119**
Current assets				
Cash and cash equivalents	6	1,051	848	994
Receivables	7	75	43	35
Inventory	8	18	23	18
Prepayments	7	59	25	67
Total current assets		1,203	939	1,114
Non-current assets				
Property, plant and equipment	9	299	340	320
Intangible assets	10	70	186	148
Capital work in progress	9, 10	89	_	_
Total non-current assets		458	526	468
Total assets		**1,661**	**1,465**	**1,582**
Current liabilities				
Payables	11	237	120	165
Employee entitlements	13	212	260	246
Total current liabilities		449	380	411
Non-current liabilities				
Lease incentive	12	32	34	52
Total non-current liabilities		32	34	52
Total liabilities		**481**	**414**	**463**
Net assets		**1,180**	**1,051**	**1,119**

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

Statement of cash flows

for the year ended 30 June 2018

	Actual 2018 $000	Budget 2018 $000	Actual 2017 $000
CASH FLOWS FROM OPERATING ACTIVITIES			
Cash was provided from			
Receipts from the Crown	4,970	4,970	4,970
Receipts from other revenue	224	203	190
Interest received	39	27	35
Cash was applied to:			
Payment to suppliers	1,479	1,281	1,335
Payments to employees	3,525	3,784	3,689
Net Goods and Services Tax	37	(1)	(8)
Net cash flows from operating activities	**192**	**136**	**179**
CASH FLOWS FROM INVESTING ACTIVITIES			
Cash was applied to			
Purchase of property, plant and equipment and intangibles	136	300	70
Cash was provided from			
Sale of property, plant and equipment and intangibles	(1)	–	–
Net cash flows from investing activities	**135**	**300**	**70**
Net increase/(decrease) in cash held	57	(164)	109
Plus opening cash	994	1,012	885
Closing cash balance	**1,051**	**848**	**994**
Cash and bank	**1,051**	**848**	**994**

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 2018

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 revenue and expenses

The year-end reported surplus is significantly different from the budgeted deficit of $68k. This is primarily due to the following:

Other revenue (up on budget by $62k)

Additional income has been received for the development of a Policy e-learning module, for attendance at the Privacy Forum in May 2018 and interest on cash balances which have ended the year higher than budget mainly as a result of lower than budgeted expenditure.

Staff expenses (down on budget by $284k)

There have been a number of staff vacancies as a result of staff departures during the year. Some of these have been in senior positions and, as a result, salary expenditure has been significantly less than budget.

Contract services (up on budget by $94k)

Additional costs in this area are mainly as a result of contractors being brought in to cover for staff vacancies as noted above. Other significant costs in this area have included assessment work to support the Office's IT environment upgrade.

Depreciation and amortisation (down on budget by $29k)

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

Other operating expenses (up on budget by $125k)

The two main areas which are over budget for the year are recruitment (over by $73k) as a result of the staff vacancies noted above, and telephones (over by $56k) as a result of the decision to make use of an external call centre for enquiries from November 2017.

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 (2017: $nil).

Other revenue breakdown

	Actual 2018 $000	Actual 2017 $000
Other grants received	187	161
Privacy Forum	52	–
Seminars and workshops	13	3
Interest revenue	40	35
Total other revenue	**292**	**199**

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 schemes and are recognised as an expense in the statement of comprehensive revenue and expenses as incurred.

Breakdown of staff costs and further information

	Actual 2018 $000	Actual 2017 $000
Salaries and wages	3,395	3,544
Employer contributions to defined contribution plans	97	105
Other staff expenses	38	25
Increase/(decrease) in employee entitlements	(34)	33
Total staff expenses	**3,496**	**3,707**

Employees' remuneration

The Office of the Privacy Commissioner is a Crown entity and is required to disclose certain remuneration information in its annual reports. The information reported is the number of employees receiving total remuneration of $100,000 or more per annum. The table below has been produced, in $10,000 bands to preserve the privacy of individuals.

Total remuneration and benefits	Number of employees	
	Actual 2018 $000	Actual 2017 $000
$100,000 – $109,999		2
$110,000 – $119,999	2	2
$120,000 – $129,999		
$130,000 – $139,999	1	1
$140,000 – $149,999	1	
$150,000 – $159,999	1	1
$160,000 – $169,999	2	1
$170,000 – $179,999	1	
$180,000 – $189,999		2
$190,000 – $199,999		
$310,000 – $319,999		
$320,000 – $329,999	1	1

No redundancy payments were made in the year. (2017: $nil)

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

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 2017 to 30 June 2018.

Name	Position	Amount 2018	Amount 2017
John Edwards	Privacy Commissioner	329,719	321,894

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.

Critical judgements in applying accounting policies

Grant expenditure

During the 2016 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 have been approved since then. The conditions included milestones and specific requirements. The Office of the Privacy Commissioner accounted for the related grant expenses when evidence of meeting these milestones was received from the recipient.

There was no grant expenditure made in 2018 (2017: $12k).

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 2018 $000	Actual 2017 $000
Fees paid to auditors:		
External audit – current year	30	30
Promotion costs:		
Website development expenses	25	32
Privacy Forum	58	7
Other marketing expenses	42	16
Total promotion expenses	**125**	**55**
Depreciation and amortisation:		
Furniture and fittings	74	72
Computer equipment	36	34
Office equipment	6	6
Intangibles	78	73
Total depreciation and amortisation	**194**	**185**
Rental expense on operating leases	417	411
Contract services	177	84
Other operating expenses:		
Computer maintenance/licences	152	138
Staff travel	143	131
Staff development	40	33
Grant expenditure	–	12
Research related	–	14
Recruitment	109	30
Litigation	5	–
Utilities	138	79
Other	175	184
Total other operating expenses	**762**	**621**

Operating leases as lessee

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

	Actual 2018 $000	Actual 2017 $000
Not later than one year	385	382
Later than one year and not later than five years	444	830
Later than five years	–	–
Total non-cancellable operating leases	**829**	**1,212**

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 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 2018 $000	Actual 2017 $000
Opening balance	1,119	1,043
Net (deficit)/surplus	61	76
Closing balance	**1,180**	**1,119**

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 2018 $000	Actual 2017 $000
Cash on hand and at bank	15	32
Cash equivalents – on call account	1,036	962
Total cash and cash equivalents	**1,051**	**994**

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 2018 $000	Actual 2017 $000
Receivables	75	35
Prepayments	59	67
Total	**134**	**102**

Total receivables comprise:		
GST receivable (exchange transaction)	71	34
Other receivables (non-exchange)	4	1
	75	**35**

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 (2017: $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 2018 $000	Actual 2017 $000
Publications held for sale	1	1
Publications held for distribution	17	17
Total inventories	**18**	**18**

No inventories are pledged as security for liabilities (2017: $nil) and no inventories were written down (2017: $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 revenue and expenses.

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 the 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 revenue and expenses.

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 revenue and expenses, 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 programmes;
- 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 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**
Balance at 1 July 2017	715	327	59	1,101
Additions	70	21	5	96
Disposals	–	(53)	–	(53)
Balance at 30 June 2018	**785**	**295**	**64**	**1,144**
Accumulated depreciation and impairment losses				
Balance at 1 July 2016	395	238	42	675
Depreciation expense	72	34	6	112
Disposals	0	(6)	0	(6)
Balance at 30 June 2017	**467**	**266**	**48**	**781**
Balance at 1 July 2017	467	266	48	781
Depreciation expense	74	36	6	116
Elimination on disposal	–	(52)	–	(52)
Balance at 30 June 2018	**541**	**250**	**54**	**845**
Carrying amounts				
As at 30 June and 1 July 2017	**248**	**61**	**11**	**320**
At 30 June 2018	**244**	**45**	**10**	**299**

There are no restrictions over the title of the Privacy Commissioner's property, plant and equipment, nor are any pledged as security for liabilities.

Capital commitments

The Privacy Commissioner has capital commitments of $34k for the year 2017/18 (2017: $nil). This relates to the purchase of computers ordered in June 2018.

Work in progress

The capital work in progress figure includes $18k for server hardware purchased as part of the IT environment upgrade. These were still being worked on as at 30 June 2018.

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 revenue and expenses.

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 licence. Some of these only have a two 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 capitalised interactive website tools comprise of two interactive databases that went live in mid-2016 and four interactive e-learning tools. 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 addition, there were two further interactive tools included in Work in Progress as at 30 June 2018.

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

- the effect of technological change on systems and platforms
- 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 three 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:

	Aquired software $000	Interactive tools $000	Total $000
Cost			
Balance at 1 July 2016	108	147	255
Additions	–	57	57
Disposals	–	–	–
Balance at 30 June 2017	**108**	**204**	**312**
Balance at 1 July 2017	108	204	312
Additions	–	–	–
Disposals	(36)	–	(36)
Balance at 30 June 2018	**72**	**204**	**276**
Accumulated depreciation and impairment losses			
Balance at 1 July 2016	80	11	91
Amortisation expense	18	55	73
Disposals	–	–	–
Balance at 30 June 2017	**98**	**66**	**164**
Balance at 1 July 2017	98	66	164
Amortisation expense	10	68	78
Disposals	(36)	–	(36)
Balance at 30 June 2018	**72**	**134**	**206**
Carrying amounts			
At 30 June and 1 July 2017	10	138	148
At 30 June 2018	**–**	**70**	**70**

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 $97k for the development costs associated with the Cloud environment and Objective (Management Information System). (2017: $26k).

Work in progress

The Capital Work in Progress figure includes $22k for Cloud related development work, $9k for Objective development work and $40k for the development of 2 interactive tools which were not ready to go live as at 30 June 2018.

Note 11: Payables

Accounting policy

Creditors and other payables are recorded at the amount payable.

Breakdown of payables

	Actual 2018 $000	Actual 2017 $000
Payables under exchange transactions		
Creditors	139	43
Accrued expenses	78	76
Lease incentive	20	20
Income received in advance	–	26
Total payables under exchange transactions	**237**	**165**
Payables under non-exchange transactions		
Other payables (GST)	–	–
Total payables under non-exchange transactions	–	–
Total creditors and other payables	**237**	**165**

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 2018 $000	Actual 2017 $000
Lease incentive	32	52
Total non-current liabilities	**32**	**52**

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 2018 $000	Actual 2017 $000
Current employee entitlements are represented by:		
Accrued salaries and wages	63	68
Annual leave	149	178
Total current portion	**212**	**246**
Current	212	246
Non-current	–	–
Total employee entitlements	**212**	**246**

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 at the time of moving into the premises.

The Auckland lease is up for renewal in July 2019. At balance date, the Privacy Commissioner has not formally decided whether to continue with the lease or find new office accommodation in Auckland. 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 (2017: $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 party 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 2018	Actual 2017
Total salaries and other short-term employee benefits	1,125,000	1,125,000
Full-time equivalent members	6	6

Key management personnel include all Senior Managers and the Privacy Commissioner who together comprise the Senior Leadership Team (SLT). One member of SLT left during the year but this position has since been filled.

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:

	2018 $000	2017 $000
FINANCIAL ASSETS		
Loans and receivables		
Cash and cash equivalents	1,051	994
Receivables (excluding prepayments and taxes receivables)	4	1
Total loans and receivables	**1,055**	**995**
FINANCIAL LIABILITIES		
Financial liabilities at amortised cost		
Payables (excluding income in advance, taxes payable, grants received subject to conditions and lease incentive)	217	119
Total financial liabilities at amortised cost	**217**	**119**

Appendices

Appendix A
Processes and services

Dispute resolution

Our Investigations and Dispute Resolution team forms the regulatory side of the Office's functions. The team investigates complaints from the public about interferences with individuals' privacy.

An interference with privacy occurs when an agency has breached a privacy principle and caused the complainant significant harm, such as negative physical, emotional or financial effects. 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:
- whether the Privacy Act covers the issue
- whether the respondent agency is responsible
- the level of harm that the breach caused.

We can compel agencies to produce documents to meet with complainants. We cannot compel complainants or respondents to accept settlement terms and we cannot award damages. However, our view is an important indication of whether there's been an interference with privacy.

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, the complainant can take their case to the Human Rights Review Tribunal.

In some exceptional circumstances, we may refer a case to the Director of Human Rights Proceedings. They can then choose to bring the case before the Tribunal.

Policy

Our Policy team provides advice to 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.

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 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 help make privacy easy. A key part of this is our online training. We have worked with education experts to build online courses about various aspects of privacy.

We respond to enquiries from journalists in traditional media and the public on social media.

Appendix B
Information matching 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.

There are three levels of programme compliance:

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 and Tax Administration Act 1994, s.82 Compliance	Compliance
1. IR/ACC Levies and Compensation To identify Accident Compensation Corporation (ACC) levy payers, and to calculate and collect premiums and residual claims levies. Inland Revenue (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 Ministry of Social Development (MSD) entitlement may have changed because they are receiving ACC payments, and to assist MSD in the recovery of outstanding debts. ACC disclosure to MSD: ACC selects individuals who have either: • claims where there has been no payment made to the claimant for six weeks (in case MSD needs to adjust its payments to make up any shortfall) • current claims that have continued for two months since the first payment, or • current claims that have continued for one year since the first payment. For these people, ACC provides MSD with the full name (including aliases), date of birth, address, IR number, ACC claimant identifier, payment start/end dates and payment amounts.	

Births, Deaths, Marriages, and Relationships Registration Act 1995, s.78A	Compliance
4. BDM (Births)/IR Newborns Tax Number To enable birth information to be confirmed in order to allocate an IR number to a new-born child. Births, Deaths and Marriages (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 and to compile mortality statistics. BDM disclosure to Ministry of Health (MoH): BDM provides child's names, gender, date of birth, place of birth, ethnicity, and parents' names, occupations, date of birth, place of birth, address(es) and ethnicities. BDM also indicates 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, date of birth and place of birth, birth registration number and full name of both mother and father. The death details include the full name, gender, date of birth, date of death, 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 NZ Deaths Register covering the 12 weeks prior to the extraction date. The information includes full name at birth, full name at death, gender, date of birth, date of death, 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 NZ Deaths Register covering the six months prior to the extraction date. The information includes full name at birth, full name at death, gender, date of birth, date of death, 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, date of birth, date of death, home address, death registration number and spouse's details.	
10. BDM (Deaths)/MoH NHI and Mortality Register To verify and update information on the NHI and to compile mortality statistics. BDM disclosure to MoH: BDM provides full name (including name at birth if different from current name), 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, date of birth, date of death, 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 NZ Deaths Register covering the 12 weeks prior to the extraction date. The information includes full name at birth, full name at death, gender, date of birth, date of death, place of birth, and number of years lived in New Zealand (if not born in New Zealand).	

13. BDM (Deaths)/NZTA Deceased Driver 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 New Zealand Transport Agency(NZTA): BDM provides death information for the fortnight prior to the extraction date. The death details include the full name (including name at birth if different from current name), gender, date and place of birth, date of death, home address and death registration number.

14. BDM (Marriages)/MSD Married Persons Benefit Eligibility

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 date of birth and addresses, and registration and marriage dates.

15. BDM/DIA(Citizenship) 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, date of birth, place of birth and parents' full names.

16. BDM/DIA(Passports) 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 for 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 extraction date. The name change details include the full name at birth, former full name, new full name, date of birth, 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 (DIA): 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, and parents' full names and birth details. Citizenship (DIA) 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 database 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 (DIA) disclosure to INZ: Citizenship provides information from the Citizenship database 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 admitted, 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 and Immigration Act 2009, s.294	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 extraction 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 which other countries, with superannuation reciprocity agreements with New Zealand, an individual may be eligible to claim superannuation payments from.

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 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 IR 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).

Not compliant – minor technical issues
A programming error resulted in IR not removing some individuals from the list of persons of interest. As a result, IR received information about some of these individuals, but took no action on that information.

27. 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 IR 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, IR number and date, time and direction of travel.

Not compliant – minor technical issues

1. A programming error resulted in IR not removing some individuals from the list of persons of interest. As a result, IR received information about some of these individuals, but took no action on that information.
2. IR sends a notice to people with student loans who are identified as having been out of the country for 140 days to warn them of the criteria for retaining their eligibility for the interest waiver. This notice is sent in advance of the date which triggers a change in their eligibility and therefore does not meet the conditions of a section 103 notice of adverse action. IR are considering their options to address this obligation.

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 IR 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).

Not compliant – minor technical issue
A programming error resulted in IR not removing some individuals from the list of persons of interest. As a result, IR received information about some of these individuals, but took no action on that information.

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 Ministry of Education (MoE): StudyLink provides MoE with the student's name(s) (in abbreviated form), date of birth, IR 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 name, date of birth, gender, address, school(s) employed at, number of half days worked, registration number (if known), and MoE employee number.

Education Council disclosure to MoE: The Education Council provides full name, 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 residency requirements, so their names may be removed from the roll.

INZ disclosure to the Electoral Commission (EC): INZ provides full name (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 database with the electoral roll so that people who are qualified to vote but have not enrolled may be invited to enrol. Citizenship (DIA) 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. Passports (DIA) 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, or to keep the core information contained in an EIC accurate and up to date.

Births disclosure to IVS: Child's names, gender, date of birth, place of birth, country of birth, 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, date of birth, place of birth, 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.

Motor Vehicle Sales Act 2003, s.122 and s.123	Compliance

39. 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

40. 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

41. 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, s.19 and Social Welfare (Reciprocity with Australia) Order 2002	Compliance

42. 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, s.19 and Social Welfare (Reciprocity with Malta) Order 2013	Compliance
43. 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 MSD client number.	

Social Welfare (Reciprocity Agreements, and New Zealand Artificial Limb Service) Act 1990, s.19 and Social Welfare (Reciprocity with the Netherlands) Order 2003	Compliance
44. 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 number. Netherlands disclosure to MSD: SVB responds with the SVB reference number.	
45. 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
46. 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, IR 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, IR number, employer's name, address, email and phone contact details, and employment commencement and cessation dates. **Replaced by an AISA from 31 August 2017**	
47. 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, IR 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, IR number, MSD client number, employer's name, address, email and phone contact details, and employment commencement and cessation dates. **Replaced by an AISA from 31 August 2017**	

Tax Administration Act 1994, s.83	Compliance
48. 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 IR 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. **Replaced by an AISA from 31 August 2017**	

Tax Administration Act 1994, s.84	Compliance

49. 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 IR number of people (and their spouse, if applicable) who are receiving WfFTC payments.

MSD disclosure to IR: For the matched records, MSD supplies the IR number, the date that WfFTC payments started and the amount paid.

Replaced by an AISA from 31 August 2017

Tax Administration Act 1994, s.85A	Compliance

50. 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.

Not compliant – minor technical issue:
A programming error resulted in IR sending incorrect information to Justice. Justice sent 3,448 adverse action letters in error. The programme was suspended until the error was corrected. Letters of apology were sent to the affected individuals by IR.

Tax Administration Act 1994, s.85G	Compliance

51. 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 IR 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. Each child's full name and date of birth are also included.

Not compliant – minor technical issue:
The letter that IR sends individuals about suspension of payments does not fully meet the notice requirements in section 103(1B) of the Act as it does not advise individuals that they have five working days to challenge the suspension.

We remain satisfied with the safeguards that IR has in place to address instances of incorrectly ceased entitlements.

Replaced by an AISA from 31 August 2017

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		
BDM/Citizenship – Citizenship Application 30 November 2017	Efficiency and security	Timely delivery of data
BDM/Passports – Passport Application 30 November 2017	Efficiency and security	Timely delivery of data
Citizenship/Passports – Passport Eligibility 30 November 2017	Efficiency and security	Timely delivery of data
Citizenship/Births – Citizenship by Birth 30 November 2017	Efficiency and security	Timely delivery of data
Inland Revenue		
BDM (Deaths)/IR – Deceased Taxpayers 25 September 2017	Efficiency and security	Timely delivery of data
Ministry of Justice		
IR/Justice Fines – Defaulters Tracing 7 March 2017	Efficiency and security	Timely delivery of data
Ministry of Social Development		
Netherlands SVB/MSD – General Adjustment 30 May 2018	Efficiency and security	Enhanced security measures
Justice/MSD – Warrants to Arrest 14 July 2017	Efficiency and security	Satisfactory audit result
Customs/MSD – Arrivals and Departures 15 September 2017	Efficiency and security	Timely delivery of data

Appendix C
Independent Auditor's Report

To the readers of the Privacy Commissioner's financial statements and performance information for the year ended 30 June 2018

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 43 to 62, that comprise the statement of financial position as at 30 June 2018, 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 5, 6, and 31 to 42.

In our opinion:

- the financial statements of the Privacy Commissioner on pages 43 to 62:
  - present fairly, in all material respects:
    - its financial position as at 30 June 2018; and
    - its financial performance and cash flows for the year then ended; and
  - comply with generally accepted accounting practice in New Zealand in accordance with Public Benefit Entity Standards Reduced Disclosure Regime.
- the performance information on pages 5, 6, and 31 to 42:
  - presents fairly, in all material respects, the Privacy Commissioner's performance for the year ended 30 June 2018, 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; and
      - 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.
  - complies with generally accepted accounting practice in New Zealand.

Our audit was completed on 31 October 2018. 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 they determine is necessary to enable them 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 1 to 4, 7 to 30, and 63 to 76 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

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

www.privacy.org.nz

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