

PRIVACY COMMISSIONER

Annual Report 2019



Annual Report of the Privacy Commissioner

for the year ended 30 June 2019

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 2019



John Edwards
Privacy Commissioner
October 2019

Introduction	1
Key points	3
Working towards our strategic goals	5
Report on activities	7
Law reform	8
Dispute resolution	9
Codes of practice	15
Policy	16
Outreach	18
International	19
Enquiries and education	20
Breach notifications	22
Information matching	23
Office and functions	25
Independence and competing interests	26
Reporting	27
Staff	27
EEO profile	28
Finance and performance report	29
Statement of responsibility	30
Statement of performance	31
Statement specifying comprehensive income	32
Cost of service statement for the year ended 30 June 2019	33
Output class 1: Guidance, education and awareness	35
Output class 2: Policy and research	37
Output class 3: Information sharing and matching	39
Output class 4: Compliance	41
Statement of accounting policies for the year ended 30 June 2019	43
Statement of comprehensive revenue and expenses for the year ended 30 June 2019	45
Statement in changes of equity for the year ended 30 June 2019	46
Statement of financial position as at 30 June 2019	47
Statement of cash flows for the year ended 30 June 2019	48
Notes to the financial statements for the year ended 30 June 2019	49
Appendices	63
Appendix A – Processes and services	64
Appendix B – Information matching programme compliance	65
Appendix C – Auditor’s Report	77

Introduction

The past year involved several major shifts in both the domestic and international privacy and data protection landscape.

New Privacy Act

The new Privacy Bill was introduced to Parliament in March 2018 and has been gradually working its way through the legislative process. It is expected to pass in late 2019. The new legislation will be the most substantial change in New Zealand privacy regulation for more than 25 years and there will be considerable work for our Office in preparing agencies and the public for that shift.

In July 2018, the Privacy Commissioner appeared before the Justice Committee to present the Office's submission on the Privacy Bill. Our Office has continued to support Ministry of Justice officials with advice on various aspects on the Bill, including issues raised by the Privacy Commissioner and other submitters. The Justice Committee reported the Privacy Bill back to Parliament on 13 March 2019 and the Bill had its second reading shortly after the end of this reporting period.

Investigation into the Ministry of Social Development

Our Office completed an inquiry into the Ministry of Social Development's (MSD) use of its compulsory information collection powers under section 11 of the Social Security Act 1964 to collect "any information" about a person on a benefit in order to assess their entitlements.

The inquiry found that while pursuing instances of benefit fraud, MSD had systematically misused its investigatory powers and failed in its obligations under the Privacy Act 1993. In doing so, MSD had unjustifiably intruded on the privacy of many beneficiaries and others.

The report made five recommendations, including that MSD immediately cease its blanket application of the 'prejudice to the maintenance of the law' exception when issuing section 11 notices. Following our report and recommendation, MSD changed its approach to high risk fraud investigations.

Christchurch mosque attacks and the Christchurch Call

The terrorist attack in Christchurch on 15 March 2019 had an enormous impact on New Zealand society. Our Office contributed to the public discussions following the attack in calling Facebook to account for its inadequate safeguards to prevent harmful online content. We also participated in meetings relating to the Christchurch Call to eliminate terrorists and violent extremist content online. This will involve ongoing policy work for our Office. We will be providing advice on the Government's proposals resulting from the attack, including the establishment of a gun register.

New Zealand's EU adequacy status

In December 2012, the European Commission recognised that New Zealand's privacy law provided 'adequate' privacy protections to meet European standards. This privilege is shared by only a handful of non-EU countries and provides New Zealand with a competitive trading advantage. During the year, the European Commission (EC) began a review of New Zealand's adequacy status. It is the first review since the EU's General Data Protection Regulation (GDPR) came into force. We have supported officials in replying to EC queries and requests for information.

Regulating tech platforms

2019 may be remembered as the year in which the importance of online privacy finally became mainstream. In the digital privacy space, the fallout from Facebook's Cambridge Analytica scandal, and social media platforms hosting disturbing videos of terrorist violence, were among incidents that brought an unparalleled level of public and regulatory scrutiny upon the practices of big tech companies.

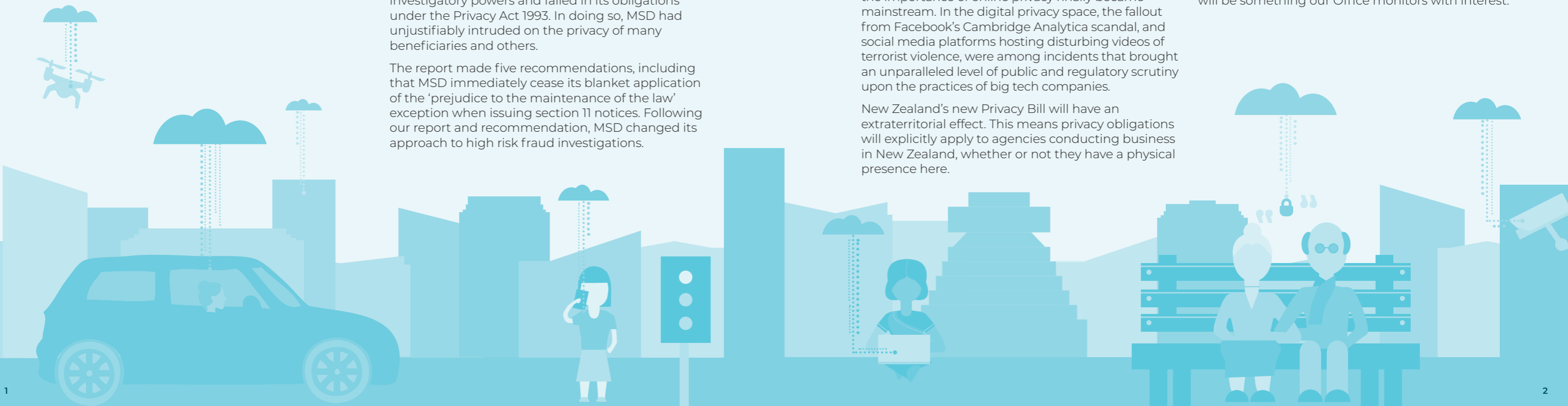
New Zealand's new Privacy Bill will have an extraterritorial effect. This means privacy obligations will explicitly apply to agencies conducting business in New Zealand, whether or not they have a physical presence here.

International privacy developments

The European Union's (EU) GDPR first came into effect on 25 May 2018 and has now been in effect for more than a year. The GDPR provides some of the most stringent rules and strongest enforcement powers globally and applies to all companies worldwide who work with personal data of EU citizens.

Reflecting the increased power and willingness of regulators to hold companies to account, unprecedented fines were levied against tech giants for data and privacy breaches during this reporting period. The Federal Trade Commission (FTC) fined Facebook a record \$7.7 billion NZD for its role in the Cambridge Analytica scandal. In Europe, the UK's Information Commissioner fined British Airways \$357 million NZD for a data breach that affected 500,000 of their customers.

The California Consumer Privacy Act (CCPA) – was passed in 2018 and will take effect on 1 January 2020. If the state of California was a country, it would be the 5th largest economy in the world. It is home to the headquarters of Facebook, Apple, Netflix, PayPal, Twitter and a host of other tech companies. The CCPA will apply to businesses, whether in the United States or abroad, that collect personal information about Californian residents. It gives Californian residents the right to know how businesses collect and handle personal information and the right to opt-out of the sale of their personal information. The implementation and industry reaction to the CCPA will be something our Office monitors with interest.



Key points

Law reform

- The Privacy Bill continued to be a significant focus for the Office.
- We worked closely with Ministry officials on outstanding issues regarding the Bill during the Select Committee process.
- The Privacy Bill was reported back by the Select Committee on 13 March 2019 and passed its second reading on 7 August 2019.

Dispute resolution

- We closed 894 investigation files.
- At the end of the reporting year, 87% of open investigation files were less than six months old.
- The total value of settlements from investigations closed by OPC in 2018/19 was \$241,104.
- We conduct regular external audits of our investigations. This year the reviewer gave 97.5% of our investigations a score of 3.5 or higher out of 5.
- We introduced compliance advice letters as an early resolution method for certain investigations.
- We referred two cases to the Director of Human Rights Proceedings.
- Twenty-three complainants took proceedings to the Tribunal themselves.
- We named one agency for non-compliance with the Privacy Act under our naming policy.

Codes of practice

- We amended the Credit Reporting Privacy Code, strengthening consumer protection.
- We conducted spot checks on the three national credit reporters using 30 mystery shoppers to ensure they were meeting their obligations under the Credit Reporting Privacy Code.

Policy

- We advised on 95 policy proposals that involved personal information and published 12 submissions.
- We supported the Christchurch Call to Eliminate Terrorist and Violent Extremist Content Online by raising the issue at international privacy conferences and providing preliminary policy advice for bills that arose following the Christchurch attack.
- We conducted an inquiry into the Ministry of Social Development's information gathering by compulsion power under the Social Security Act.

Outreach

- We gave 112 in-person presentations to a diverse range of groups.
- We hosted five PrivacyLive events in Auckland and Wellington.
- The Commissioner made visits to 10 regions around the country to speak with, and take questions from, the public and other stakeholders.

International

- In late November 2018, we hosted 38 delegates from 18 jurisdictions in Queenstown for the International Working Group on Data Protection in Telecommunications (IWGDPT) called the 'Berlin Group'.
- Immediately following this, in December 2018, we hosted the 50th Asia Pacific Privacy Authorities (APPA) forum in Wellington, focussing on opportunities for cooperation on privacy matters across the Asia Pacific region followed by the International Privacy Forum, open to privacy and data protection professionals and the general public.
- We attended the 40th International Conference of Data Protection and Privacy Commissioners (ICDPPC) in Brussels.
- We participated in monthly Global Privacy Enforcement Network (GPEEN) Pacific teleconferences with privacy authorities across the world.

Enquiries and education

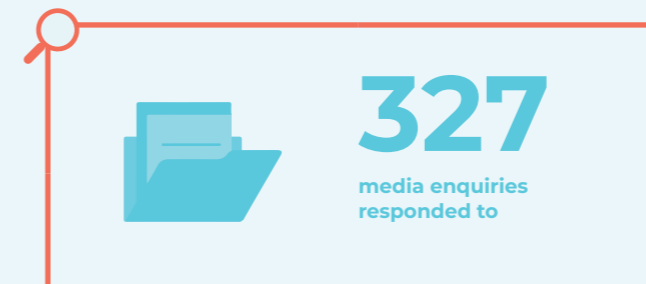
- We answered 7,947 public enquiries.
- There were 16,852 public searches made through our online FAQ service, AskUs.
- Our call centre, established during the last reporting period, responded to 4,251 call centre enquiries. The other 3,696 enquiries were handled in-house.
- We responded to 327 media enquiries.
- We awarded Air New Zealand's privacy centre with a Privacy Trust Mark, to recognise its excellence.

Breach notifications

- Agencies reported 222 breaches of the security of personal information to us.
- With the introduction of mandatory privacy breach notifications under the Privacy Bill, the number of breaches reported to us is expected to increase significantly.

Information matching

- We reviewed four information matching provisions used by Inland Revenue and recommended that they should all continue without amendment.
- There are 47 information matching programmes in operation and eight inactive programmes this year.
- Parliament passed no new information matching provisions during the year.
- Four programmes transferred to operating under Approved Information Sharing Agreements.



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. 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 reap benefits from people's personal information, and new technologies make that information more valuable and easier to access.

New Zealand needs citizens and consumers to 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

We continued to raise the public visibility of privacy through participation in media interviews regarding topical privacy issues, answering the public's questions through our online FAQ section, AskUs, and promoting and receiving a greater number of hits on our website and social media channels.

Our Investigations and Dispute Resolution team continued to provide independent and effective dispute resolution services via phone and online for individuals with privacy complaints. We improved our dispute resolution process through the introduction of compliance advice letters.

We used our naming policy under the Privacy Act to name the Sensible Sentencing Trust for hosting an innocent man's photo on their website for two years because he shared the same name as a convicted paedophile.



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 applied for and were granted funding from the International Association of Privacy Professionals ANZ Legacy Fund. This will enable us to support innovative privacy research projects for the benefit of New Zealand through our Privacy Good Research Fund.

New Zealand's new Privacy Bill will require all agencies to notify us if they breach someone's privacy. We have continued to work closely with our counterparts in Australia and elsewhere to learn about their experiences implementing mandatory breach notification regimes and to apply those lessons to assist OPC and the wider community to prepare for the Privacy Bill.

During the last reporting period, we introduced our Privacy Trust Mark scheme which recognises excellence in privacy-friendly products or services. Since that time, we have awarded three Trust Marks with several others currently under consideration. This scheme encourages agencies to keep privacy in mind as they innovate and advance their practices.



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 continued to work on the Privacy Bill, aiming to strengthen privacy protection for individuals and help ensure that agencies comply with the law and good personal information practices.

We released our online training module *Privacy for Policy Makers*, developed in partnership with the Government Chief Privacy Officer. Our e-learning modules received strong uptake in the community.

We are regularly contacted by agencies for on-the-spot guidance regarding hot-button privacy issues. This year we strengthened our relationships with the likes of the Privacy Foundation, The Southern Initiative, Consumer NZ, the Government Chief Privacy Officer, the Government Chief Data Steward, the Domain Name Commission, Internet NZ, Oranga Tamariki and others.

We visited 10 regions around New Zealand to engage with the public on privacy issues and recent developments.

We hosted multiple major international privacy events including the International Working Group on Data Protection in Telecommunications (Queenstown, November 2018), the 50th Asia Pacific Privacy Authorities (APPA) Forum (Wellington, December 2018) and the International Privacy Forum (Wellington, December 2018).



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 July 2018, the Privacy Commissioner appeared before the Justice Committee to present his submission on the Privacy Bill. During this reporting period, we continued to support Ministry of Justice officials with advice on various aspects of the Bill, including issues raised by the Privacy Commissioner and other submitters.

We continued to work closely with Ministry officials on outstanding issues and technical drafting matters, to support advice for the Select Committee for the Departmental Report in November 2018, and provided supplementary advice to the Justice Committee in February 2019. This work included consideration of the extraterritorial application of the Bill, cross border provisions, the new privacy breach notification scheme, and other technical matters.

The Justice Committee reported the Privacy Bill back to Parliament on 13 March 2019 and it passed its second reading on 7 August 2019.



7 AUG

The Privacy Bill passes its second reading



Dispute resolution

Our dispute resolution team is at the coalface of our organisation. They are usually the first point of contact for the public's privacy queries and complaints.

This reporting year we closed 894 investigation files, a 26% increase on the 2017/2018 period. 87% of investigation files were closed within six months, which fell slightly short of meeting our KPI of 90% of files closed within six months.

OPC regularly engages external auditors to conduct reviews of our investigations. Files reviewed by the auditor for the period 1 July-31 December 2018 received an average score of 4.2 out of a possible 5. Files closed between 1 January-30 June 2019, received an average of 4.1. The combined average score for this reporting period was 4.14. 97.5% of our investigators files scored 3.5 or higher.

Figure 1
Age of open complaint files as at 30 June 2019

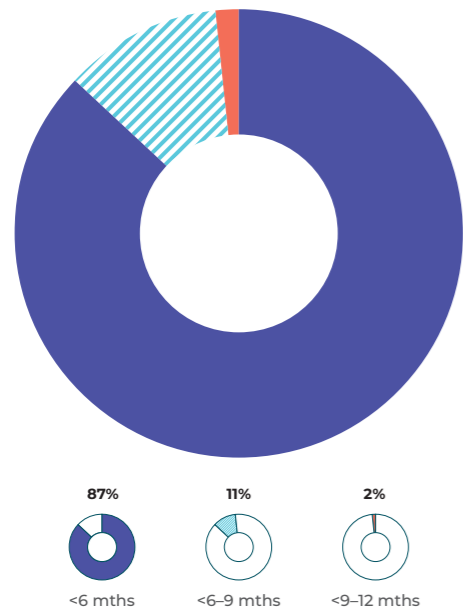
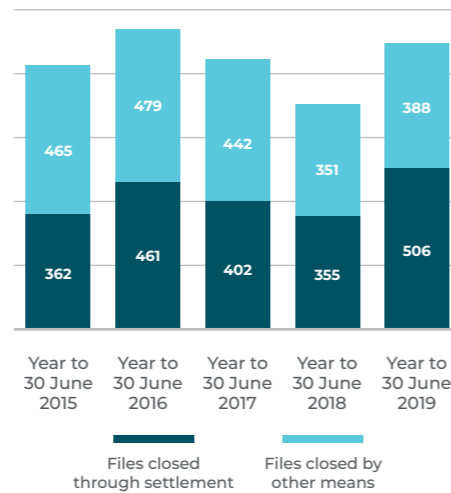


Figure 2
Result of complaint file reviews



97.5%
of investigations assessed by an independent reviewer received a score of 3.5 or higher

Case examples

CASE ONE

Sensible Sentencing Trust falsely labels man as paedophile

A man's photograph was wrongly listed on the Sensible Sentencing Trust's (SST) 'Offender Database' beside a description of a convicted paedophile for two years before being taken down. The convicted paedophile had the same first and last names as the man, but their middle names were different. The man's image received 574 unique views before he was alerted to its existence. He informed SST of the error and the image was removed. He subsequently complained to our Office.

Under principle 8 of the Privacy Act, agencies must take reasonable steps to check personal information is accurate, complete, relevant, up-to-date and not misleading before using or disclosing that information. SST said that an unknown member of the public had submitted the photo and that their website was maintained by volunteers. Despite already being told by our Office to improve compliance in 2014 over another privacy case, SST did not know who had approved the photo for

publication. Volunteers were not provided with privacy training and SST had no process to verify that the photo was accurate before uploading it to the website.

The SST's failure to check the accuracy of its information implicated an innocent person for a terrible crime, tarnished his reputation, caused him emotional harm and put him at risk of violence. Our investigations are almost always confidential, but we applied our naming policy in this instance to publicly identify the SST to inform the public of its bad practice and remind other agencies of the importance of their privacy obligations. Two years earlier, SST signed a settlement with the Director of Human Rights Proceedings for breaching principles 6, 8 and 11 of the Privacy Act and had agreed to provide privacy training to its staff.

Due to the significance of this case, the Privacy Commissioner referred it to the Director of Human Rights Proceedings.

CASE TWO

Law firm wanted \$19,000 for information request

A man requested his law firm give him access to his information. Principle 6 of the Privacy Act provides individuals with a right to access personal information held by an agency. If a response is not given within 20 working days, there is an automatic interference with the requester's privacy. The firm failed to respond within this timeframe. When they eventually got back to their client, they told him it would cost \$19,000 to provide his information. The man complained to our Office.

Section 35 of the Privacy Act states that agencies may charge to provide information but sets limits as to what is reasonable to recoup the costs of photocopying, printing and staff time in carrying out administrative tasks. The law firm said it had followed Ministry of Justice guidelines on charging under the Official Information Act and the total came to \$19,175.

The Privacy Commissioner exercised the discretion provided to him by section 78 of the Privacy Act and set the charge at the reasonable cost of purchasing an 8GB USB stick – at \$7.99 from Warehouse Stationery. The law firm refused to back down on the \$19,000 charge. We closed the file, advising the client that he had the right to take the case to the Human Rights Review Tribunal. The client then filed proceedings with the Tribunal.

When the law firm was informed the matter was before the Tribunal, the man told our Office the law firm delivered two boxes of files to him, which he copied and returned.



CASE THREE

Transport sector employer disclosed employee's pregnancy to workmates

An employee working in a transport safety role complained to our Office after her employer disclosed her pregnancy to colleagues without permission. The complainant said she had informed her employer of her pregnancy as required by the law governing her profession. The complainant had taken sick leave and the complainant's manager told other staff that he couldn't disclose why the employee was off. He instead provided hints until one staff member reached the conclusion that the absent staff member was pregnant.

The woman lodged a complaint directly with the employer who commissioned an internal investigation. The internal investigation concluded that the manager had breached principles 5, 10 and 11 of the Privacy Act and violated a duty of care to his employee. The employer refused to accept liability and the woman complained to our Office. Our view was that the manager had interfered with the complainant's privacy and should consider making an offer of compensation to her. This case was settled by the employer paying the employee \$10,000.



CASE FOUR

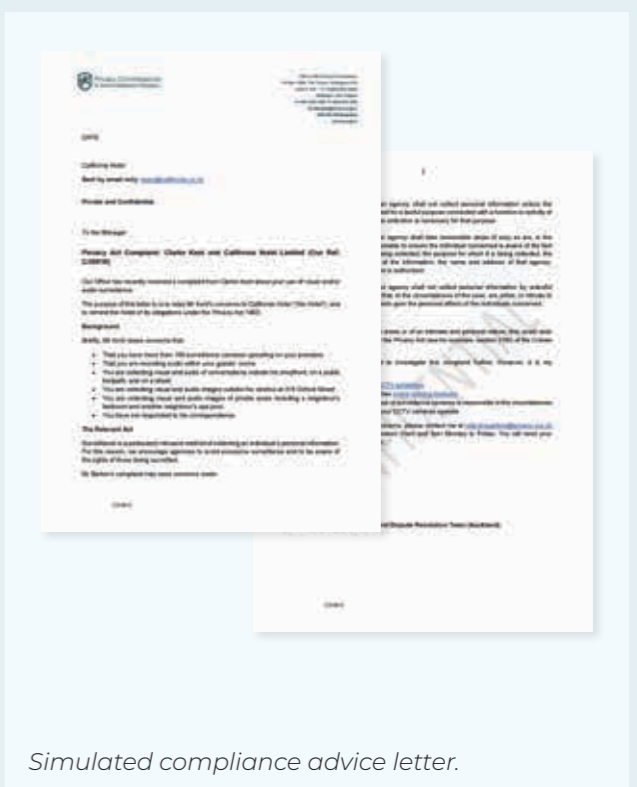
NZ Post employee complains about audio recording made on delivery vehicles

A NZ Post delivery driver complained to us about audio recordings made by cameras installed on a "Paxster" electric delivery vehicle. The man discovered that calls and conversations with members of the public were being recorded during his delivery run. He was not aware the cameras could record audio and was shocked and upset when he realised this. Principle 1 of the Privacy Act says that personal information must only be collected for lawful purposes connected with what the agency does. NZ Post stated that their delivery drivers were not acting in a personal capacity while completing their delivery work. We explained that under the Privacy Act 'personal information' had a wide definition and includes any information that is about an identifiable individual. Although the man was working, the camera was also recording his personal conversations. NZ Post argued audio recordings were necessary to investigate incidents or accidents that occur during delivery rounds.

Principle 3 says that when collecting information, agencies must make people aware of the fact that information is being collected, the purposes for which it is being collected and the intended recipients. We found that because NZ Post had not made the delivery man aware that the cameras were recording audio, they had breached principle 3. Principle 4 says that personal information should not be collected by an agency by unlawful means or means that are unfair or unreasonably intrusive. Our view was that the need to investigate possible incidents in NZ Post delivery vehicles had to be balanced against employees' rights to privacy and dignity. It would be unreasonably intrusive to record audio the entire time a Paxster is being driven. We facilitated a mediation and the parties reached a settlement. NZ Post changed its policy and no longer uses cameras with an audio function on its Paxster vehicles.

Compliance Advice Letters

During the past year, our Office introduced a new resolution option to deal with complaints that do not meet the threshold to conduct a full investigation. For example, we can only investigate things that appear to be an interference with privacy. This means a breach of an information privacy principle and some harm or loss or significant injury to feelings. Where a complaint appears to disclose a breach of an information privacy principle but does not reach the threshold of harm, we can use a compliance advice letter. This communicates a complainant's privacy issues and reminds agencies of their obligations under the Privacy Act. Our Office receives a broad variety of complaints and some of these, while potentially problematic, do not show evidence of serious harm being caused. Many agencies in New Zealand are small and may be unaware of their obligations under the Privacy Act. Compliance advice letters give our investigators another option to address privacy concerns raised by the public without going through the full investigation process. Below are two examples of cases we addressed using a compliance advice letter.



Simulated compliance advice letter.

CASE FIVE

Church outreach staff pass on man's details to other church members

A man invited several church outreach members who had called at his house to come in for an informal chat about religion. Sometime later, he was visited by a different group from the same church who greeted him at the door by using his first name. This shocked the man who was informed by the visitors they had been given notes about him from the other church members he had interacted with. The man made an access request to the church to see what information they held about him. After he received no response he complained to our Office.

We contacted the church with a compliance advice letter questioning what information they collected from the public. We explained that if the church was collecting personal information from people, they needed to inform them what information they were gathering and for what purpose it was being used. The church had collected basic information regarding people's names and marriage status. It apologised to the man and noted down not to visit his home again. We declined to investigate further as there was no evidence of harm.

CASE SIX

Mother concerned about multiple security cameras on neighbouring residential property

We received a complaint from a woman concerned about the presence of several high-tech security cameras on a neighbouring rural property in a small community. The complainant had several concerns, including that the neighbour's cameras were interrupting the quiet enjoyment of many in the community of walking along one of the community's few main roads without being captured by the cameras. In general, complaints of this nature fall under section 56 of the Privacy Act. It states that the privacy principles do not apply where information is collected for the purposes of or in connection with, an individual's personal, family or household affairs.

The respondent said the cameras had been installed on his property for his safety after an incident where he had been assaulted by another neighbour. He said that the cameras complied with all local by-laws. Our compliance advice letter noted the complainant's worries about the security cameras. We reminded the respondent that if he was operating a business from his home, he may be subject to principles 1, 3, and 4 of the Privacy Act. We encouraged him to avoid excessive surveillance, to be aware of the rights of those being surveilled and to additionally place signage to alert residents and visitors about the presence of cameras.

Figure 3
Top complaints by agency

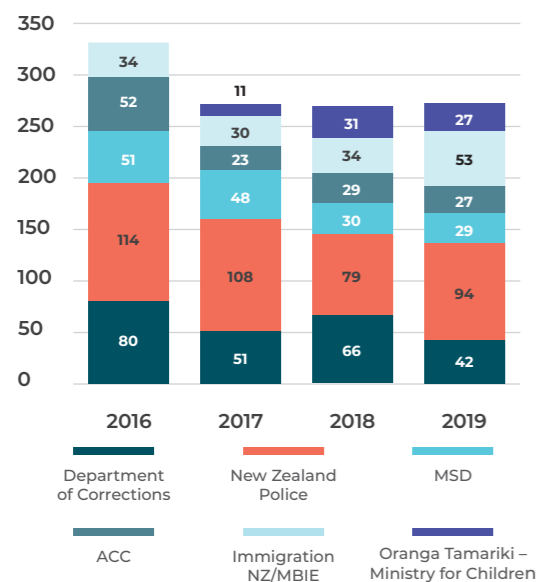
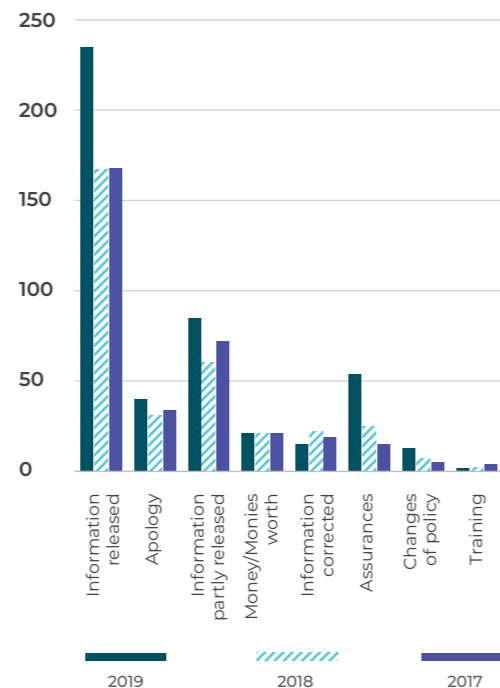


Figure 4
Settlement outcomes




\$241,104
Total amount paid in settlements through the Dispute Resolution process

Human Rights Review Tribunal

We aim to resolve most complaints during 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 referred to the Tribunal

This year we referred two cases to the Director. The Director has filed proceedings in one of those cases.

Twenty-three complainants took proceedings to the Tribunal themselves, without a referral from us (29 did so in the previous year).

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 eight Privacy Act cases this year. Four of those were dismissals, with no interference with privacy found.

Of the four decisions that found an interference with privacy, two awarded damages to the plaintiffs – one for \$70,000 (*Director of Human Rights Proceedings v Slater* [2019] NZHRRT 19) and the other, combined damages of \$28,000 (*Tapiki and Eru v NZ Parole Board* [2019] NZHRRT 5).

In terms of legal developments, the Slater case concerned the limits on the scope of a key exemption from the Privacy Act. The Tribunal affirmed the statutory phrase “news activity” is to be understood as “news activity which is conducted responsibly”. The Tribunal also held that the publication of personal information must itself also be a news activity in order to qualify for the exemption.

A further 18 cases filed in the Tribunal were withdrawn before they went to hearing.

Naming

We operate a naming policy in accordance with section 116(2) of the Privacy Act. Under the policy an agency may be named in a public report where, on balance, we considered that the agency ought to be named for the purpose of giving effect to the Privacy Act.

In the 2018/19 year, we published the name of one agency, the Sensible Sentencing Trust (SST), after an investigation concluded that the SST had interfered with a man’s privacy by falsely labelling him as a convicted paedophile on its website (see case note on page 10).

In 2014, we warned the SST to improve its compliance with the Privacy Act. As the case note demonstrates, they had failed to do so. We took the decision to publicly name SST to warn the New Zealand public of the SST’s continuously negligent, cavalier, and dangerous approach to privacy.

Codes of practice

At the start of the year there were six codes of practice in force. During the year we amended the Credit Reporting Privacy Code.

Amendments to the Credit Reporting Privacy Code

The Credit Reporting Privacy Code provides the framework for New Zealand's comprehensive credit reporting regime. Credit reporters collect and share information about individuals' credit history, which is used to help credit providers make decisions about whether to issue loans or extend credit to borrowers. Comprehensive credit reporting is designed to provide individuals greater access to credit by allowing positive as well as negative credit reporting.

We amended the Credit Reporting Privacy Code in November 2018, following a public submission process. The new provisions tightened the credit code, enforcing stricter controls on credit reporters. The amendments also clarify the requirements around individual consent processes and enhance the rights of New Zealanders to get access to their credit reports and credit scores quickly and for free. The amendment came into force in phases throughout 2019.

Compliance checks for the Credit Reporting Privacy Code

Between October 2018 and February 2019, we conducted spot checks using 30 mystery shoppers on the three credit reporting companies Centrix, Equifax, and illion. The aim was to assess whether credit reporters complied with access rules and limits on charging (as at 30 March 2019). We also checked whether they provided free credit reports as quickly as possible.

The findings were published in May 2019 and showed that credit reporters often failed to meet the five working day timeliness rules for expedited reports. While credit reporters were generally providing free reports within the 20 working day time frames, we recommended that since information is easily retrievable, credit reporters should strive to provide reports as quickly as practicable.



Policy

Our policy team works with agencies 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.

In an external audit of a representative sample of policy files from the last year, 92% of files assessed met or exceeded our quality standard of 3.5 out of 5. The auditor noted that our work was typically "exemplary of good practice" and it compared well with other agencies.

This year we advised on 95 policy proposals, mostly from government agencies, that involved personal information. We also published 12 submissions and 9 office research projects.

Inquiry into the Ministry of Social Development's Exercise of section 11 (Social Security Act 1964) and compliance with the Code of Conduct

We conducted an inquiry into the Ministry of Social Development's (MSD) exercise of its information gathering powers under the Social Security Act. The inquiry found MSD was acting in a manner inconsistent with its legal requirements, resulting in infringements of individual privacy. The Ministry is required to seek information from individuals directly unless doing so would cause a prejudice to the maintenance of the law. The inquiry found MSD had been intentionally bypassing the requirement to seek information from individuals directly and instead, had compelled third parties to provide information without the individuals' knowledge.

Examples of privacy infringements included:

- Failing to ask beneficiary clients for information before seeking it from a third party leading to inaccurate assessments of the information;
- Overly broad requests leading to the provision of unnecessary and sensitive information;
- Disproportionate and inappropriate requests for information (in some cases, every text message sent and received by an individual over lengthy time periods).

We released our inquiry report in May 2019. The Ministry accepted all our recommendations and has instituted a process to ensure consideration is made on a case by case basis before information gathering powers are used to seek information from individuals or third parties. The Minister has asked the Ministry to undertake an urgent review of their legislation to ensure that it is fit for purpose.

Christchurch mosque attacks and the Christchurch Call

The Christchurch Call to Action to Eliminate Terrorist and Violent Extremist Content Online is a cross-government and international initiative led by

the New Zealand Government, following the 15 March mosque shootings in Christchurch. The Call included engagement across government, civil society, academics and the wider community. We have long held concerns regarding the ways social media companies collect and use people's personal information. Algorithms on these digital platforms harness personal information to deliver increasingly personalised content to users. While one algorithm may recommend music to someone based on their tastes, another may feed users extreme content, contributing to polarisation and divisiveness.

The Privacy Commissioner contributed to the public discussion regarding the role of social media in the 15 March attack. He was interviewed widely by domestic and international media, criticising Facebook for failing to have adequate safeguards in place to prevent the use of its platform for the broadcast and dissemination of harmful content.

We expect our Office to have ongoing policy work as a result of the Christchurch Call in relation to new firearms legislation, and have met and continue to work with the Royal Commission of Inquiry into the Attack on Christchurch Mosques. The new Privacy Bill will also have extra-territorial application, holding overseas agencies doing business in New Zealand accountable for their handling of New Zealanders' personal information.

Recommended repeal of unused information matching provisions

Following our review of Government information matching provisions showing many were never used, we issued a report recommending 22 information matching provisions be repealed. Once an information matching provision is enacted, section 106 of the Privacy Act requires the Privacy Commissioner to review the operation of the provision to consider whether the authority conferred should be continued and whether any amendments to the provision are necessary or desirable. The Commissioner stated the unused information matching provisions did not deliver their intended benefits to society and continuing parliamentary authorisation of these privacy intrusive measures was unjustified. This highlights the importance of a thorough and robust examination of the business case for proposed programmes that take up parliamentary time, and potentially undermine privacy protections, without necessarily promising realistic public benefits.

Submissions on Bills

Criminal cases DNA review

The Law Commission is currently reviewing the use of DNA in criminal investigations (involving the collection, use and storage of DNA samples and profiles in the criminal justice context). Our submission to the Law Commission noted the significant privacy implications of DNA collection in law enforcement. We stressed that clear legislative parameters and appropriate checks and safeguards are necessary to ensure that intrusions into the privacy of the individual are not unwarranted, and to limit any unintended adverse consequences.

We noted that the Law Commission's review is an opportunity to address outstanding issues and to strengthen the substantive and procedural safeguards, while ensuring that Police have appropriate access to DNA to support investigations of sufficiently serious criminal offending. We commented that an important reform is to affirm in statute that an individual's genetic material (DNA) is "personal information" as defined in the Privacy Act. This will ensure that the privacy principles underpin the collection, analysis, use and disclosure of DNA samples, as well as the DNA profiles derived from them.

We support the Law Commission's proposal for reform of the Criminal Investigations (Bodily Samples) Act, including establishing independent oversight of the operation and use of the DNA databanks. The Office is represented on the Expert Advisory Group and has continued to participate in EAG discussions regarding proposals for a new legislative regime for the use of DNA in criminal investigations.

Modernisation of the Tax Administration Act

In August 2018, the Privacy Commissioner made a submission to the Finance and Expenditure Committee on the Taxation (Annual Rates for 2018-19, Modernising Tax Administration, and Remedial Matters) Bill.

Our submission focused on improving new provisions in the Tax Administration Act covering the collection, use, and disclosure of revenue information. There were six recommendations in the submission, designed to enhance transparency and privacy considerations, and strengthen privacy safeguards. Areas of focus in our submission included the regular collection of bulk information by Inland Revenue and the collection and on-sharing of personal information obtained by Inland Revenue using mandatory collection powers. The submission supported new provisions that provided for Inland Revenue to disclose information to protect health and safety. All of our recommendations were either fully or partially implemented in the revised Bill.

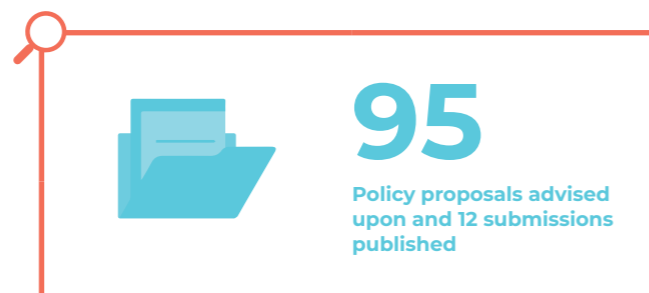
Mental health and addiction inquiry

In November 2018, the Government Inquiry into Mental Health and Addiction published its report, *He Ara Oranga*. The Commissioner met with the Inquiry Chair during the Inquiry to discuss the feedback they had received from submitters, regarding privacy being used inappropriately as a reason for withholding information from family and whānau. We collated a selection of existing guidance material and advised the Chair that we would be happy to participate in revision of those materials, as well as working with professional groups to encourage understanding of appropriate information sharing in the mental health and addiction context.

Following the release of the report, and the Government's response, we have offered our assistance in updating guidance on sharing information and partnering with families and whānau. This will enable health care providers to communicate appropriately while upholding the rights (including privacy rights) of the person with mental health or addiction needs. The Government's response acknowledged the role of the Privacy Commissioner in this area and indicated it would continue to involve us in ongoing work.

Police vetting

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 beginning the policy development work to draft a statutory framework for the Police Vetting Service. We have a role in assessing draft legislation and are working with Police to ensure the privacy rights of individuals are upheld.



Outreach

We have an ongoing commitment to provide opportunities for groups to meet and discuss privacy issues with us in person. During the past year, we gave a total of 112 presentations (up 18% on last year) to a diverse range of audiences.

Regional visits

The Privacy Commissioner frequently travels to regional centres to strengthen our connections and promote our resources.

The visits provide the Commissioner with the opportunity to speak and take questions from the public about the latest developments in privacy, and present to DHBs, local government, NGOs, and other groups.

In the reporting period, the Commissioner visited:

- Timaru, Oamaru, Dunedin (August 2018)
- Palmerston North (August 2018)
- Rotorua and Whakatāne (October 2018)
- New Plymouth (November 2018)
- Dannevirke (February 2019)
- Christchurch and Waimakariri (February 2019).

PrivacyLive

Our PrivacyLive speaker series continued throughout the reporting period.

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

- Andrew Chen, New boundaries of camera-based surveillance – 18 September 2018 (Wellington)
- Law Commission on DNA and Crime – 10 October 2018 (Auckland)
- Jason Cronk, Embedding Privacy by Design – 26 October 2018 (Wellington)
- Law Commission DNA and Crime – 14 March 2019 (Wellington)
- Anelka Phillips, Your DNA is Only a Click Away – 20 June 2019 (Auckland).

We livestream these events to make sure they are accessible to those who are unable to make it in person.

Sir Bruce Slane Memorial lectures

In November 2018, we hosted two lectures in Auckland and Wellington to mark the 25th anniversary of the Privacy Act and Sir Bruce Slane's singular contribution to the development of privacy law in New Zealand, on 6 November 2018 (Wellington) and 8 November 2018 (Auckland). Presented by the now Chief Justice, Dame Helen Winkelmann, the lectures were well attended by the judiciary and wider legal community.

Privacy Week

Privacy Week is an annual event (held in May) 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. This year we hosted five PrivacyLive events during Privacy Week in Auckland, Wellington and Christchurch.

This year's Privacy Week highlights included:

- Presentations on the impact of grief journalism during Pike River and the impact of GDPR on New Zealand businesses
- A privacy-themed art exhibition at Vincent's Art Workshop in Wellington
- Launching a privacy for policy makers e-learning module
- Producing Privacy Week posters available to stakeholders around the country
- Working with The Southern Initiative on an online "callout" campaign to find out the views of young Māori and Pasifika people.

Privacy Trust Mark

We want to help New Zealanders make informed choices about privacy-friendly products and services. The Privacy Trust Mark was launched in May 2018 with the aim to give consumers assurances that a product or service has been designed with privacy in mind.

When assessing applications from organisations, we look at factors such as:

- Has privacy been embedded into the design?
- Is privacy a core value of the organisation?
- Does the product or service demonstrate end-to-end security?
- Is the customer in control of their personal information?
- Is there an ongoing commitment to improve privacy practice?

To date we have awarded three Trust Marks. The first was for Internal Affairs' RealMe service, the second was for Trademe's Transparency reporting and in May this year, we awarded Air New Zealand a Trust Mark for its privacy centre.



International

We participated in key international privacy forums during the year:

- the Asia Pacific Privacy Authorities Forums (APPA)
- the International Conference of Data Protection and Privacy Commissioners (ICDPPC)
- the International Working Group on Data Protection in Telecommunications (IWGDPT) “Berlin Group”

Asia Pacific Privacy Authorities Forums (APPA)

APPA is the principal forum for privacy and data protection regulators in the Asia Pacific region and meets twice a year. In December 2018, we hosted the 50th APPA Forum in Wellington, focusing on opportunities for cooperation on education and enforcement activities across the Asia Pacific region. We welcomed representatives from 19 Asia-Pacific privacy regulators and authorities and had discussions regarding:

- Fair and ethical data processing using artificial intelligence
- The right to have yourself de-linked from personal information that’s public information (“right to be forgotten”)
- Privacy developments in Africa
- Children’s privacy
- Algorithmic transparency.

In May this year, we also attended and participated in the 51st APPA Forum in Tokyo, Japan. Some of the main topics discussed were:

- Cross border data transfers
- Privacy trust marks
- Open banking
- Terrorism and social media.

International Privacy Forum

Immediately following last December’s APPA, our Office also held an International Privacy Forum at the Intercontinental Hotel in Wellington. Unlike APPA, the International Privacy Forum was open to anyone who worked in the privacy and data protection areas who wished to learn more about the current global trends and concerns. The forum featured a presentation from the UK’s Information Commissioner, Elizabeth Denham. She highlighted key issues in New Zealand’s privacy landscape as well as the General Data Protection Regulation and their impact on New Zealand businesses which trade with the European Union.

International Conference of Data Protection and Privacy Commissioners (ICDPPC)

We attended the 40th gathering of the ICDPPC held in October 2018 in Brussels. The Conference featured heads of state and CEOs and had a focus on ethics. We proposed a resolution that was adopted, ensuring the Conference census is conducted every three years. Apple CEO Tim Cook challenged the tech industry for using personal information against consumers, saying it was being weaponised “with military efficiency”. While in Europe, the Commissioner also attended workshops in Zurich regarding the protection of children in a connected world and in Paris regarding mandatory data breach reporting.

“Berlin Group” – 64th meeting of the International Working Group on Data Protection in Telecommunications (IWGDPT)

Our Office hosted the 64th meeting of the “Berlin Group” in Queenstown on 29-30 November 2018. The meeting involved 38 delegates from 18 jurisdictions. Discussions focussed on artificial intelligence, location tracking, smart devices, and data portability.

Other international activities

Global Privacy Enforcement Network (GPEN)

GPEN continues to be a key means of connecting with our counterparts in enforcement. We participate in monthly GPEN Pacific teleconferences. In 2018, we jointly managed and coordinated the GPEN Sweep with the Information Commissioner’s Office, UK. The topic of the Sweep was privacy accountability and was designed to assess how well organisations implemented the concept of privacy accountability into their own internal privacy programmes and policies. The Sweep was carried out by 18 GPEN members around the world, contacting a total of 667 organisations.

Enquiries and education

This year we responded to 7,947 public enquiries. This represents a 15% drop from the last reporting period. We believe fewer enquiries are coming to us directly because we continue to develop our AskUs knowledge base.

Of the total, 4,251 enquiries came through the call centre. Our aim is to enable the call centre to deal with straightforward questions, leaving staff in-house to provide more tailored assistance.

AskUs

AskUs is the privacy FAQ section of our website. It is one of the main ways our Office answers privacy queries from the public. During the last reporting year, we recorded a total of 16,852 AskUs searches. This is comparable to the number of queries received last year.

The top three most searched questions during this reporting period were:

1. What is personal information?
2. Can I record someone without telling them?
3. Are there rules regarding where CCTV cameras can be placed?

We received an increase in the number of questions during Privacy Week in May.

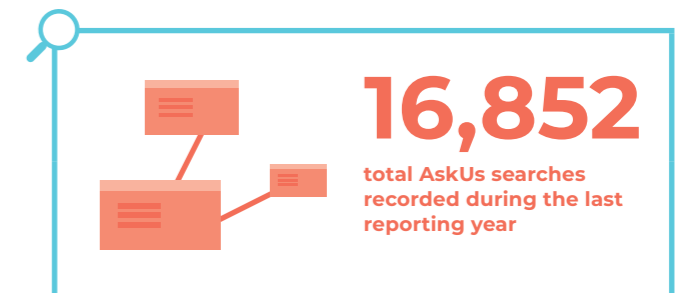
Call centre

We initially trialled the call centre during the last reporting period. The call centre staff take approximately 300-350 calls per month, and this is having a positive impact on our workflows. About 50 of the most complex matters a month are referred to the dispute resolution team for a response.

Live Chat

During the last reporting year, we introduced a live chat tool on our website to give the public a further channel to engage with staff directly about their Privacy Act queries. One of the values of live chat is knowing what information people are seeking in real-time. We will continue to monitor Live Chat’s effectiveness as a tool over the coming year.

Figure 5
Unique website visitors



Media

In the past year we received 327 media enquiries. This was similar to the 345 enquiries received in the previous year, and still significantly up from 2016/17.

Several high-profile issues generated media enquiries during this reporting year. Some examples include the revelations about Facebook and Cambridge Analytica, the use of facial recognition technology in New Zealand, overcollection of information by landlords, the Privacy Bill, the Christchurch Call and several significant data breaches.

Online learning modules

This year we released two new e-learning modules. In August 2018, we introduced *Health ABC*, which received significant engagement and in May 2019, we released *Privacy for Policy Makers*. The policy module was developed in association with the Government Chief Privacy Officer.

With the addition of the new courses, the Office now offers nine education modules. They have good uptake with more than 1,000 people completing a module each month. Over 22,000 people have completed our e-learning courses.

Breach notifications

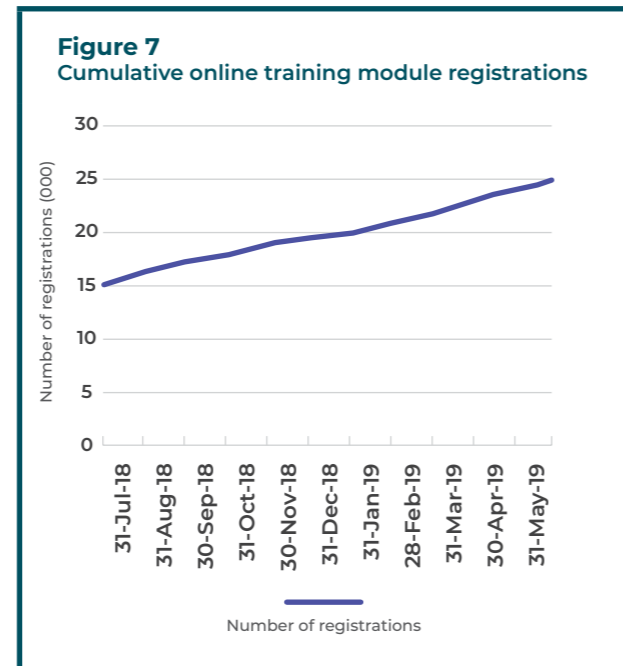
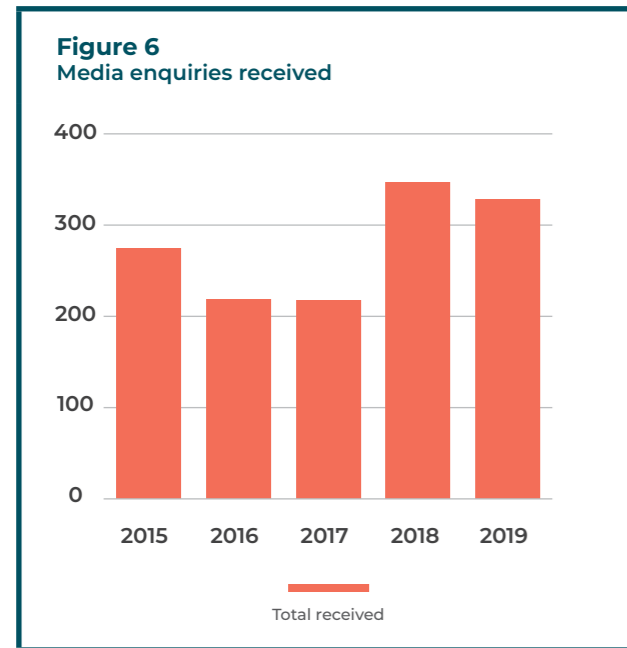
We receive voluntary breach notifications from a variety of public and private sector agencies. We encourage this because we can guide agencies on how they should respond to breaches, and how they can stop them from happening again.

The notifications also help us identify common privacy issues and risks, and we use the lessons learned from these breaches in developing education resources or FAQs.

This year agencies reported 222 breaches to us. Ninety-five of those notifications were from public agencies and the other 127 from private agencies.

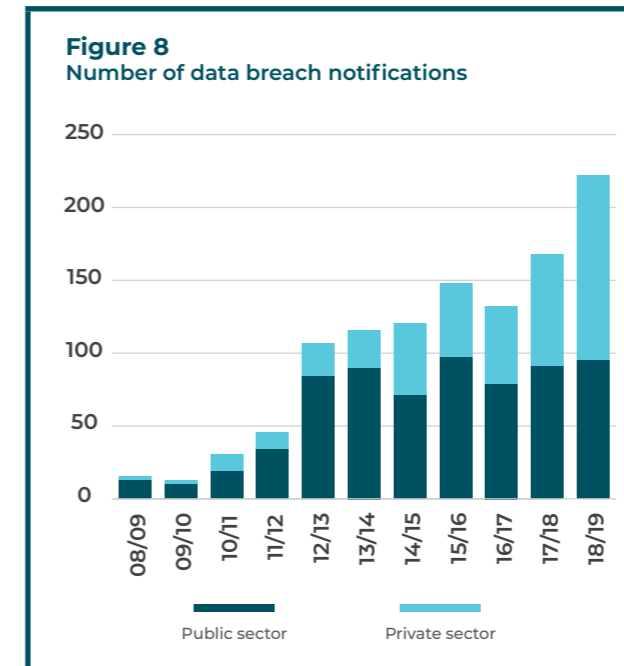
Getting ready for mandatory breach notifications

The Privacy Bill before Parliament will 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.



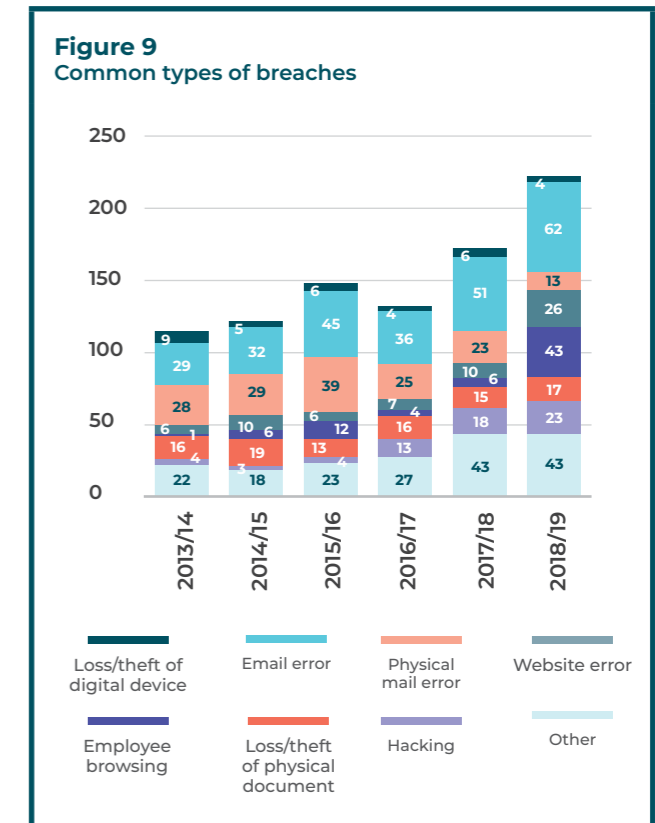
Landlord Guidance

This guidance outlines what information should and should not be collected by landlords when deciding whether someone will make a suitable tenant. These guidelines are aimed at landlords in the private sector. They were released during Privacy Week in May and a revised version was released at the end of the reporting period.




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 is the most common cause of privacy breaches.



We are preparing for the additional demands the mandatory reporting requirement will place on the Office by looking at the experience of our international counterparts.



222

breaches reported to us, 95 of those notifications were from public agencies and the other 127 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. We then recommend whether a provision should continue, be amended or be cancelled.

This year we reviewed four information matching provisions used by Inland Revenue (IR) and recommended that they should all continue without amendment.

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

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

This provision allows IR to match information with the Department of Internal Affairs, enabling parents to apply for a tax number for their child when they register the birth.

Customs and Excise Act 1996, s 280H (with the passing of the Customs and Excise Act 2018 this provision was replaced by s 306)

This provision allows IR to match information with the New Zealand Customs Service to receive alerts when an individual with an outstanding loan balance enters New Zealand.

Student Loan Scheme Act 2011, s 208

This provision enables IR to operate an information match with the New Zealand Customs Service to be advised of travel movements of individuals with student loans so that IR can assess eligibility for interest write-offs.

Customs and Excise Act 1996, s 280K (with the passing of the Customs and Excise Act 2018 this provision was replaced by s 307)

This provision allows IR to match information with the New Zealand Customs Service to be alerted when parents in serious default of their child support obligations enter or leave New Zealand.

Changes in authorised and operating programmes

There were 47 information matching programmes in operation, and eight programmes that were inactive in 2018/19. We assessed eight programmes as non-compliant with the requirements intended to protect individuals affected by these programmes. Aside from the Department of Internal Affairs' failure to provide the reporting required to monitor and assess four of their matches, other issues have been resolved in consultation with the Office.

New provisions and programmes:

Parliament passed no new information matching provisions during the year. No new programmes commenced operation during the year.

Programmes suspended:

Immigration New Zealand did not operate its programmes with the DIA for Deaths and Citizenship Information. (Births, Deaths, Marriages and Relationships Registration Act 1995 s 78A and Citizenship Act 1977, s 26A).

The Ministry of Business, Innovation and Employment did not operate its 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 its programme with the DIA for birth records but is working on re-starting this programme and incorporating Name Change and Death information. (Births, Deaths, Marriages and Relationship Registration Act 1995, s 78A).

The Ministry of Justice did not operate its programme with Immigration New Zealand for arrival and departure information to help locate people who owe fines because of the significant manual effort involved and the comparatively low benefits from the programme. The Ministry 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. MSD advise that Australia's concerns with Australian privacy law have been resolved and therefore they may resume operating the programme. (Social Security Act 2018, s 380 and Social Welfare (Reciprocity with Australia) Order 2017).

MSD also did not need to use the provision to allow Inland Revenue to respond to tax information enquires from the Netherlands social welfare authorities, as no requests were received from the Netherlands. (Social Security Act 2018, s 385(3) and Tax Administration Act 1994 s 85B).

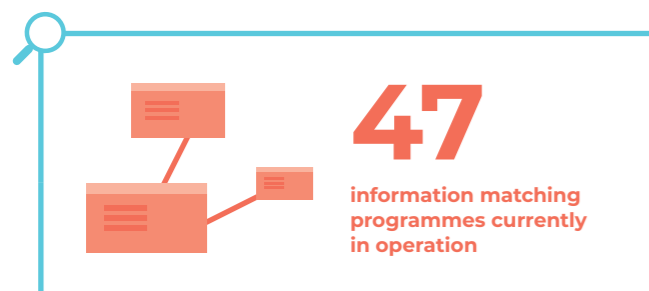
MSD did not use powers to require information for matching from employers under Clauses 6 and 7 of Schedule 6 of the Social Security Act 2018 (previously s 11A of the Social Security Act 1964).

Programmes ceasing:

Four of the current information matches between different functions of the Department of Internal Affairs are being replaced by an Approved Information Sharing Agreement. The "Information Sharing Agreement between the Department of Internal Affairs and the Registrar-General, Births, Deaths and Marriages" was authorised by an Order-in-Council on 17 December 2018 (Privacy (Information Sharing Agreement between Department of Internal Affairs and Registrar-General) Order 2018 (2018/275)). DIA is in the process of modifying their work processes and systems. When these changes are complete, it will operate the information sharing under the AISA.

- Citizenship/DIA Passports
- BDM/DIA Passports
- BDM Births & Marriages/Citizenship Applications
- Citizenship/BDM Citizenship by Birth

The Customs/MSD Arrivals and Departures match has been replaced by an information sharing agreement authorised by an Order-in-Council on 15 April 2019 (Privacy (Information Sharing Agreement between Ministry of Social Development and New Zealand Customs Service) Order 2019 (2019/75)).



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 (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 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 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 the 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 factors
- 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 an inclusive culture.

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

Our recruitment policies, including advertising, comply with the good employer expectations of Diversity Works New Zealand, of which we are a member.

We have formal policies regarding bullying, harassment, and the provision of a safe and healthy workplace. Staff have ready access to external support through our employee assistance programme.

Workplace gender profile

as at 30 June 2019

Role	Women		Men		Total
	Full-time	Part-time	Full-time	Part-time	
Commissioner			1		1
Senior managers	2		2		4
Team and unit managers	4		1		5
Investigations and Dispute Resolution	7	1	2		10
Administrative support	5	1			6
Policy	4		2		6
Communications			3		3
Legal	2				2
Total	24	2	11	0	37

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 2019.



J Edwards
Privacy Commissioner
31 October 2019



G F Bulog
General Manager
31 October 2019



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 2019 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	5,096	4,970
Other revenue	227	251
Total revenue	5,323	5,221

The appropriation received by the Privacy Commissioner, equals the government's actual expenses incurred in relation to the appropriations, which is a required disclosure from the Public Finance Act.

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 operating grant target included \$126k towards Privacy Act Implementation costs. At the time the budget was set, the assumption was that the law reform would progress to enactment within this financial year and this funding would then be made available in the year to June 2019. This did not occur but it is expected to be received in the next financial year.

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 1.9% of the total Vote Justice Non-Departmental Output Expenses Appropriation for 2018/19. The total expenses in the year are \$5,425k as set out in the cost of service statement on page 33.

Cost of service statement

for the year ended 30 June 2019

As set out in the 2018/19 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 2019 \$000	Budget 2019 \$000	Actual 2018 \$000
OUTPUT CLASS 1: GUIDANCE, EDUCATION AND AWARENESS			
Resources employed			
Revenue	818	795	839
Expenditure	748	750	721
Net Surplus/(Deficit)	70	45	118
OUTPUT CLASS 2: POLICY AND RESEARCH			
Resources employed			
Revenue	1,900	2,053	1,955
Expenditure	2,098	2,199	2,063
Net Surplus/(Deficit)	(198)	(146)	(108)
OUTPUT CLASS 3: INFORMATION SHARING/MATCHING			
Resources employed			
Revenue	783	697	789
Expenditure	729	615	704
Net Surplus/(Deficit)	54	82	85
OUTPUT CLASS 4: COMPLIANCE			
Resources employed			
Revenue	1,720	1,778	1,679
Expenditure	1,850	1,831	1,713
Net Surplus/(Deficit)	(130)	(53)	(34)
TOTALS			
Resources employed			
Revenue	5,221	5,323	5,262
Expenditure	5,425	5,395	5,201
Net Surplus/(Deficit)	(204)	(72)	61

The following tables set out the 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 business 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 business. 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 2018/19	Achieved 2017/18
Quantity			
Number of people completing education modules on the online system.	3,500	Achieved 10,326 people have completed e-learning modules in the year to 30 June 2019.	Achieved – 4,845
Presentations at conferences and seminars.	90	Achieved – 112	Achieved – 96
Public enquiries received and answered.	7,500 ¹	Achieved – 7,947 Public enquiries are externally driven and will fluctuate between years.	Achieved – 9,147
Media enquiries received and answered.	200	Achieved – 327	Achieved – 345
Quality			
Website contains all current published guidance from the Privacy Commissioner, and additional resources to support compliance with the Act.	Achieved	Achieved	Achieved

¹ This target was included within the Non-Departmental Output Expenses – Services from the Privacy Commissioner appropriation and was the same as the SPE target.

Measure	Estimate	Achieved 2018/19	Achieved 2017/18
Quantity			
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 – 96%²	Achieved – 94%
Timeliness			
Respond to all enquiries within two working days.	100% ³	Not achieved – 92%	Substantially achieved – 95%

² 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 50 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.

³ 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 2018/19	Achieved 2017/18
Quantity			
The number of consultations, submissions and office projects completed in the year.	150	Not achieved – 116 The number of consultations is demand driven through external organisations.	132 ⁴
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 has hosted 3 international events during the year in New Zealand – the Berlin Group Meeting, APPA Forum and International Privacy Forum.	Achieved
Quality			
The percentage of recipients of policy advice who are satisfied with the service they received from the Privacy Commissioner.	85% ⁵	Achieved – 86%⁶	Achieved – 87%
Our participation in the law reform process is valued by the Ministry of Justice.	Achieved	Achieved The Ministry of Justice described the input of OPC to be "high quality" and further said "your expert opinion and operational input is particularly valuable."	Achieved
The percentage of externally reviewed policy, information sharing and information matching files that are rated 3.5 out of 5 or better for quality.	85% ⁷	Achieved – 92% Based on findings from an independent review of a sample of files closed in the year.	Substantially achieved for policy files – 83% Achieved for information sharing and matching files – 100% (In the prior year these were measured separately)

⁴ The reporting on this measure was split out in the prior year across 3 separate targets. The 132 is made up of 107 proposals, 14 submissions and 11 office projects.

⁵ This target was included within the Non-Departmental Output Expenses – Services from the Privacy Commissioner appropriation and was the same as the SPE target.

⁶ 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 22 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.

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.

Measure	Estimate	Achieved 2018/19	Achieved 2017/18
Timeliness			
The percentage of policy files where advice was delivered within agreed timeframes.	100%	Substantially achieved – 95%	Substantially achieved – 97%
Responses to requests for input into legislative reform proposals are made available within agreed timelines.	100%	Not achieved Based on the annual stakeholder survey results, 88% of law reform related respondents noted that the timeframe had been met. Only two respondents indicated that the timeframe had not been met. ⁸ Direct correspondence with the Ministry of Justice confirmed that all requests for responses for input into law reform were timely and within agreed timelines.	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. 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.

⁸ 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 16 responses to this question relating to law reform. See footnote 6 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 on how to meet their responsibilities under Part 9A and Part 10 respectively.

Output Measures

Measure	Estimate	Achieved 2018/19	Achieved 2017/18
Quantity			
The number of information matching programmes monitored under Part 10 of the Privacy Act.	50 ⁹	Achieved – 55 (47 current programmes and eight inactive programmes.)	Achieved – 58
The number of new Approved Information Sharing Agreements received for consultation under s 96O of the Privacy Act.	2	Achieved – 2	Achieved – 4
The number of formal reports produced that relate to information sharing or information matching programmes, under s 96P, 96X, 96O or 106 of the Privacy Act.	8	Not achieved – 4	Achieved – 9
The number of proposals consulted on involving information sharing or matching between government agencies, completed during the year.	30	Substantially achieved – 29	Achieved – 38

⁹ This target was included within the Non-Departmental Output Expenses – Services from the Privacy Commissioner appropriation and was the same as the SPE target.

Measure	Estimate	Achieved 2018/19	Achieved 2017/18
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 – 92%¹⁰	Achieved – 90%
Timeliness			
The percentage of information sharing and matching files where advice was delivered within agreed timeframes.	100%	Achieved – 100%	Substantially achieved – 98%

¹⁰ 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 13 responses to this question relating to information sharing/matching. See footnote 6 on page 37 for limitations

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. The online complaints lodgement system, that was introduced four years ago, has been increasingly used as a method to lodge complaints with the office. In this reporting year 43% of all complaints were lodged in this way.

We also review and amend codes of practice.

Measure	Estimate	Achieved 2018/19	Achieved 2017/18
Quantity			
Number of complaints received.	900 ¹¹	Not achieved – 793 The number of complaints received is an estimate only as it is externally driven.	Not achieved – 807
Number of data breach notifications received.	130	Achieved – 222	Achieved – 168
Quality			
The percentage of complaints files closed by settlement between the parties.	40% ¹²	Achieved – 57%	Achieved – 50%
Amendments to Codes of Practice meet all statutory requirements.	100%	Achieved Amendments were made to the Credit Reporting Privacy Code in the year following its review.	Achieved
The percentage of externally reviewed complaints investigations that are rated as 3.5 out of 5 or better for quality.	85%*	Achieved – 98% Based on the results of an external review of a sample of complaints files closed between July 2018 and June 2019.	Achieved – 95%
Recommendations following the Credit Reporting Privacy Code review are actioned.	Achieved	Achieved The first of three tranches of amendments to the Credit Reporting Privacy Code came into force on 1 April 2019.	Not applicable – this is a new measure for 2018/19.

¹¹ This target was included within the Non-Departmental Output Expenses – Services from the Privacy Commissioner appropriation and was the same as the SPE target.

¹² This target was included within the Non-Departmental Output Expenses – Services from the Privacy Commissioner appropriation and was the same as the SPE target.

Measure	Estimate	Achieved 2018/19	Achieved 2017/18
Timeliness			
The percentage of open files greater than 6 months old at the year end.	10% ¹³	Not achieved – 13% Staff turnover has impacted on the delivery of services.	Not achieved – 11%

¹³ This target was included within the Non-Departmental Output Expenses – Services from the Privacy Commissioner appropriation and was the same as the SPE target.

Statement of accounting policies

for the year ended 30 June 2019

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 2019 and were approved by the Commissioner on 31 October 2019. 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.

Standards early adopted

In line with Financial Statements of Government, the Privacy Commissioner has elected to early adopt PBE IFRS 9 *Financial Instruments*. PBE IFRS 9 replaces PBE IPSAS 29 *Financial Instruments: Recognition and Measurement*. Information about the adoption of PBE IFRS 9 is provided in Note 18.

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

The net amount of GST recoverable from, or payable to, the Inland Revenue (IR) 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 2019:

- 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 2019

	Note	Actual 2019 \$000	Budget 2019 \$000	Actual 2018 \$000
Revenue				
Crown revenue	2	4,970	5,096	4,970
Other revenue	2	251	227	292
Total income		5,221	5,323	5,262
Expenditure				
Promotion	4	120	139	125
Audit fees		32	30	30
Depreciation and amortisation	4, 9, 10	221	252	194
Rental expense		420	421	417
Operating expenses		933	753	762
Contract services		259	187	177
Staff expenses	3	3,440	3,613	3,496
Total expenditure		5,425	5,395	5,201
Surplus/(Deficit)		(204)	(72)	61
Other comprehensive revenue and expenses		-	-	-
Total comprehensive revenue and expenses		(204)	(72)	61

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 2019

	Note	Actual 2019 \$000	Budget 2019 \$000	Actual 2018 \$000
Total equity at the start of the year		1,180	1,286	1,119
Total comprehensive revenue and expenses for the year		(204)	(72)	61
Total equity at the end of the year	5	976	1,214	1,180

Explanations of major variances are provided in Note 1.

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

Statement of financial position

as at 30 June 2019

	Note	Actual 2019 \$000	Budget 2019 \$000	Actual 2018 \$000
Public equity				
General funds	5	976	1,214	1,180
Total public equity		976	1,214	1,180
Current assets				
Cash and cash equivalents	6	840	743	1,051
Receivables	7	99	26	75
Inventory	8	16	25	18
Prepayments	7	86	25	59
Total current assets		1,041	819	1,203
Non-current assets				
Property, plant and equipment	9	285	566	299
Intangible assets	10	151	208	70
Capital work in progress	9, 10	–	–	89
Total non-current assets		436	774	458
Total assets		1,477	1,593	1,661
Current liabilities				
Payables	11	269	135	237
Employee entitlements	13	220	230	212
Total current liabilities		489	365	449
Non-current liabilities				
Lease incentive	12	12	14	32
Total non-current liabilities		12	14	32
Total liabilities		501	379	481
Net assets		976	1,214	1,180

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

Statement of cash flows

for the year ended 30 June 2019

	Actual 2019 \$000	Budget 2019 \$000	Actual 2018 \$000
CASH FLOWS FROM OPERATING ACTIVITIES			
Cash was provided from			
Receipts from the Crown	4,970	5,096	4,970
Receipts from other revenue	225	193	224
Interest received	27	30	39
Cash was applied to			
Payment to suppliers	1,781	1,557	1,479
Payments to employees	3,423	3,606	3,525
Net Goods and Services Tax	(21)	(11)	37
Net cash flows from operating activities	39	167	192
CASH FLOWS FROM INVESTING ACTIVITIES			
Cash was applied to			
Purchase of property, plant and equipment and intangibles	250	590	136
Cash was provided from			
Sale of property, plant and equipment and intangibles	–	–	(1)
Net cash flows from investing activities	250	590	135
Net increase/(decrease) in cash held	(211)	(423)	57
Plus opening cash	1,051	1,166	994
Closing cash balance	840	743	1,051
Cash and bank	840	743	1,051

The GST (net) component of operating activities reflects the net GST paid and received with Inland Revenue. 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 2019

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 deficit is significantly different to the budgeted deficit of \$72k. This is primarily due to the following:

Operating Grant (down on budget by \$126k)

The \$126k Privacy Act Implementation Costs contingency funding was not received in the year. The budget had been set on the assumption that the first tranche of funding would be available in the 2019 financial year.

Staff expenses (down on budget by \$173k)

There have been a number of staff vacancies as a result of staff departures during the year. In particular, one of the senior leadership team members left and this position was disestablished. As a result, salary expenditure has been significantly less than budget.

Contract services (up on budget by \$72k)

Additional contractors were mainly brought in to cover for staff vacancies as noted above. Other significant costs included work to support the Office's IT environment upgrade which took place in October 2018 as well as work associated with the legislative reforms.

Depreciation and amortisation (down on budget by \$31k)

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

Other operating expenses (up on budget by \$180k)

The three main areas which are over budget for the year are network costs (over by \$49k), software licensing costs (over by \$41k) and telephones (over by \$20k). The increases in both network and licensing costs are mainly due to the costs associated with the IT environment upgrade that took place during the year. The telephone cost variance is due to higher than expected external call centre costs.

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

Sale 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.

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 (2018: \$nil).

Other revenue breakdown

	Actual 2019 \$000	Actual 2018 \$000
Other grants received	161	187
Forums and conferences	60	52
Seminars and workshops	0	13
Interest revenue	30	40
Total other revenue	251	292

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 2019 \$000	Actual 2018 \$000
Salaries and wages	3,302	3,395
Employer contributions to defined contribution plans	97	97
Other staff expenses	33	38
Increase/(decrease) in employee entitlements	8	(34)
Total staff expenses	3,440	3,496

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 2019 \$000	Actual 2018 \$000
\$100,000 – \$109,999		
\$110,000 – \$119,999		2
\$120,000 – \$129,999	3	
\$130,000 – \$139,999	1	1
\$140,000 – \$149,999	1	1
\$150,000 – \$159,999		1
\$160,000 – \$169,999	1	2
\$170,000 – \$179,999	1	1
\$180,000-\$189,999	1	
\$190,000-\$199,999		
\$320,000-\$329,999		1
\$330,000-\$339,999		
\$340,000-\$349,999	1	

No redundancy payments were made in the year (2018: \$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 2018 to 30 June 2019.

Name	Position	Amount 2019	Amount 2018
John Edwards	Privacy Commissioner	343,373	329,719

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 2019 (2018: nil).

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 2019 \$000	Actual 2018 \$000
Fees paid to auditors:		
External audit – current year	32	30
Promotion costs:		
Website development expenses	26	25
Privacy Forum	8	58
Conferences	61	–
Other marketing expenses	26	42
Total promotion expenses:	120	125
Depreciation and amortisation:		
Furniture and fittings	86	74
Computer equipment	33	36
Office equipment	11	6
Intangibles	91	78
Total depreciation and amortisation	221	194
Rental expense on operating leases	420	417
Contract services	259	177
Other operating expenses:		
Computer maintenance/licences	202	152
Staff travel	153	143
Staff development	84	40
Loss on disposal	2	–
Recruitment	86	109
Litigation	–	5
Utilities	221	138
Other	185	175
Total other operating expenses	933	762

Operating leases as lessee

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

	Actual 2019 \$000	Actual 2018 \$000
Not later than one year	338	385
Later than one year and not later than five years	654	444
Later than five years	169	-
Total non-cancellable operating leases	1,161	829

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 current lease on the Auckland premises expired on 31 July 2019. A new lease including reduced floor space was re-negotiated on these premises. This was signed on 30 June 2019 and is included in the above disclosure. The lease will expire in December 2025.

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 2019 \$000	Actual 2018 \$000
Opening balance	1,180	1,119
Net (deficit)/surplus	(204)	61
Closing balance	976	1,180

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 2019 \$000	Actual 2018 \$000
Cash on hand and at bank	71	15
Cash equivalents – on call account	769	1,036
Total cash and cash equivalents	840	1,051

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 an allowance for expected losses.

	Actual 2019 \$000	Actual 2018 \$000
Receivables	99	75
Prepayments	86	59
Total	184	134
Total receivables comprise:		
GST receivable (exchange transaction)	50	71
Other receivables (non-exchange)	49	4
Total	99	75

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 (2018: \$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 2019 \$000	Actual 2018 \$000
Publications held for sale	1	1
Publications held for distribution	15	17
Total inventories	16	18

No inventories are pledged as security for liabilities (2018: \$nil) and no inventories were written down (2018: \$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 2017	715	327	59	1,101
Additions	70	21	5	96
Disposals	–	(53)	–	(53)
Balance at 30 June 2018	785	295	64	1,144
Balance at 1 July 2018	785	295	64	1,144
Additions	–	78	60	138
Disposals	–	(209)	(48)	(257)
Balance at 30 June 2019	785	164	76	1,025
Accumulated depreciation and impairment losses				
Balance at 1 July 2017	467	266	48	781
Depreciation expense	74	36	6	116
Disposals	–	(52)	–	(52)
Balance at 30 June 2018	541	250	54	845
Balance at 1 July 2018	541	250	54	845
Depreciation expense	86	33	11	130
Elimination on disposal	–	(205)	(30)	(235)
Balance at 30 June 2019	627	78	35	740
Carrying amounts				
At 30 June and 1 July 2018	244	45	10	299
At 30 June 2019	158	86	41	285

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 \$nil as at 30 June 2019 (2018: \$34k).

Work in progress

The capital work in progress figure is \$nil as at 30 June 2019 (2018: \$18k for server hardware purchased as part of the IT environment upgrade).

Note 10: Intangible assets

Accounting policy

Software acquisition

Acquired computer software licences 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 six 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 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:

	Acquired software \$000	Interactive tools \$000	Total \$000
Cost			
Balance at 1 July 2017	108	204	312
Additions	–	–	–
Disposals	(36)	–	(36)
Balance at 30 June 2018	72	204	276
Balance at 1 July 2018	72	204	276
Additions	133	39	172
Disposals	(72)	0	(72)
Balance at 30 June 2019	133	243	376
Accumulated amortisation and impairment losses			
Balance at 1 July 2017	98	66	164
Amortisation expense	10	68	78
Disposals	(36)	–	(36)
Balance at 30 June 2018	72	134	206
Balance at 1 July 2018	72	134	206
Amortisation expense	29	62	91
Disposals	(72)	–	(72)
Balance at 30 June 2019	29	196	225
Carrying amounts			
At 30 June and 1 July 2018	–	70	70
At 30 June 2019	104	47	151

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 \$nil as at 30 June 2019 (2018: \$97k).

Work in progress

The Capital Work in Progress figure for 2019 is \$nil (2018: included \$22k for Cloud related development work, \$9k for Objective development work and \$40k for the development of 2 interactive tools).

Note 11: Payables

Accounting policy

Creditors and other payables are recorded at the amount payable.

Breakdown of payables

	Actual 2019 \$000	Actual 2018 \$000
Payables under exchange transactions		
Creditors	135	139
Accrued expenses	68	78
Lease incentive	20	20
Total payables under exchange transactions	223	237
Payables under non-exchange transactions		
Other payables	46	–
Total payables under non-exchange transactions	46	–
Total creditors and other payables	269	237

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 2019 \$000	Actual 2018 \$000
Lease incentive	12	32
Total non-current liabilities	12	32

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 2019 \$'000	Actual 2018 \$'000
Current employee entitlements are represented by:		
Accrued salaries and wages	64	63
Annual leave	156	149
Total current portion	220	212
Current	220	212
Non-current	-	-
Total employee entitlements	220	212

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 renewed in July 2019. At balance date, the Privacy Commissioner had renegotiated the lease terms. The "Make Good" clause was not invoked.

Other than as stated above, there are no known contingencies existing at balance date (2018: \$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 party 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 2019 \$'000	Actual 2018 \$'000
Total salaries and other short-term employee benefits	1,050	1,125
Full-time equivalent members	5	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.

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:

	2019 \$'000	2018 \$'000
FINANCIAL ASSETS		
Financial assets measured at amortised cost		
Cash and cash equivalents	840	1,051
Receivables (excluding prepayments and taxes receivable)	49	4
Total loans and receivables	889	1,055
FINANCIAL LIABILITIES		
Financial liabilities at amortised cost		
Payables (excluding income in advance, taxes payable, grants received subject to conditions and lease incentive)	203	217
Total financial liabilities at amortised cost	203	217

Note 18: Adoption of PBE IFRS 9 Financial Instruments

The only accounting policy to be updated to comply with PBE IFRS 9 is as follows:

- Note 7 Receivables: This policy has been updated to reflect that the impairment of short terms receivables is now determined by applying the expected loss model.

On the date of initial application of PBE IFRS 9, being 1 July 2018, the classification of financial instruments under PBE IPSAS 29 and PBE IFRS 9 is as follows:

	Measurement category		Carrying amount
	Original PBE IPSAS 29 category	New PBE IFRS 9 category	As at 30 June 2018 under PBE IPSAS 29 and 1 July 2018 under PBE IFRS 9 (no adjustments required)
Cash and cash equivalent	Loans and receivables	Amortised cost	1,051
Receivables	Loans and receivables	Amortised cost	4
Total financial assets			1,055

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 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 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 and 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. The Director 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 (replaced by Schedule 7 Part C subpart 2 cl 41) Compliance

1. IR/ACC Compensation

To confirm income amounts for compensation calculations.

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.



Not compliant – minor technical issues

Letters to individuals did not include specific details required by s 103 of the Privacy Act 1993. The issue has been resolved.

Accident Compensation Act 2001, s 246 and Tax Administration Act 1994, s 82 (replaced by Schedule 7 Part C subpart 2 cl 42) Compliance

2. IR/ACC Levies

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

3. 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

4. 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
<p>5. BDM (Births)/IR Newborns Tax Number</p> <p>To enable birth information to be confirmed in order to allocate an IR number to a new-born child.</p> <p>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.</p>	
<p>6. BDM (Births)/MoH NHI and Mortality Register</p> <p>To verify and update information on the National Health Index and to compile mortality statistics.</p> <p>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.</p>	
<p>7. BDM/MSD Identity Verification</p> <p>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.</p> <p>BDM disclosure to MSD: BDM provides birth and death information for the 90 years prior to the extraction date.</p> <p>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.</p>	
<p>8. BDM (Deaths)/GSF Eligibility</p> <p>To identify members or beneficiaries of the Government Superannuation Fund (GSF) who have died.</p> <p>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).</p>	
<p>9. BDM (Deaths)/IR Deceased Taxpayers</p> <p>To identify taxpayers who have died so that IR can close accounts where activity has ceased.</p> <p>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.</p> <p>Not compliant – minor technical issue</p> <p>Incorrect matches were loaded to the new system and staff were not made sufficiently aware of simple process to re-activate accounts. This issue has been corrected.</p>	
<p>10. BDM (Deaths)/MoH NHI and Mortality Register</p> <p>To verify and update information on the NHI and to compile mortality statistics.</p> <p>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.</p>	
<p>11. BDM (Deaths)/MSD Deceased Persons</p> <p>To identify current clients who have died so that MSD can stop making payments in a timely manner.</p> <p>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.</p>	
<p>12. BDM (Deaths)/NPF Eligibility</p> <p>To identify members or beneficiaries of the National Provident Fund (NPF) who have died.</p> <p>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).</p>	
<p>13. BDM (Deaths)/NZTA Deceased Driver Licence Holders</p> <p>To improve the quality and integrity of data held on the Driver Licence Register by identifying licence holders who have died.</p> <p>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.</p>	

<p>14. BDM (Marriages)/MSD Married Persons Benefit Eligibility</p> <p>To identify current clients who have married so that MSD can update client records and reassess their eligibility for benefits and allowances.</p> <p>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.</p>	
<p>15. BDM/DIA(Citizenship) Citizenship Application Processing</p> <p>To verify a parent's citizenship status if required for determining an applicant's eligibility for New Zealand citizenship.</p> <p>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.</p>	
<p>16. BDM/DIA(Passports) Passport Eligibility</p> <p>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.</p> <p>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.</p>	
<p>17. BDM/MSD Overseas Born Name Change</p> <p>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.</p> <p>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.</p>	


Citizenship Act 1977, s 26A	Compliance
<p>18. DIA (Citizenship)/BDM Citizenship by Birth Processing</p> <p>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.</p> <p>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.</p> <p>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</p>	
<p>19. DIA(Citizenship)/DIA(Passports) Passport Eligibility</p> <p>To verify a person's eligibility to hold a New Zealand passport from Citizenship database information.</p> <p>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.</p>	
Corrections Act 2004, s 180	Compliance
<p>20. Corrections/MSD Prisoners</p> <p>To detect people who are receiving income support payments while imprisoned, and to assist MSD in the recovery of outstanding debts.</p> <p>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.</p>	
Corrections Act 2004, s 181 and Immigration Act 2009, s 294	Compliance
<p>21. Corrections/INZ Prisoners</p> <p>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.</p> <p>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.</p> <p>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.</p>	
Customs and Excise Act 2018, s 306	Compliance
<p>22. Customs/IR Student Loan Alerts</p> <p>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.</p> <p>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.</p> <p>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).</p>	
<p>23. Customs/IR Student Loan Interest</p> <p>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.</p> <p>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.</p> <p>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.</p>	

Customs and Excise Act 2018, s 307	Compliance
<p>24. Customs/IR Child Support Alerts</p> <p>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.</p> <p>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.</p> <p>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).</p>	
Customs and Excise Act 2018, s 308	Compliance
<p>25. Customs/MSD Arrivals and Departures</p> <p>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.</p> <p>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.</p>	
Customs and Excise Act 2018, s 309	Compliance
<p>26. Customs/MSD Periods of Residence</p> <p>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.</p> <p>Customs disclosure to MSD: Customs provides MSD access to its CusMod system for verification of departure and arrival dates.</p>	
Customs and Excise Act 2018, s 310	Compliance
<p>27. Customs/Justice Fines Defaulters Alerts</p> <p>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.</p> <p>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.</p> <p>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.</p>	


Education Act 1989, s 226A and s 235F Compliance

28. 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

29. 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


30. 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


31. 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

32. DIA (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).
Not compliant – minor technical issue.
 The data supplied by DIA included names previously used by some individuals. The program used to extract the data has since been modified to exclude these.

33. 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.

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.

Electronic Identity Verification Act 2012, s 39 Compliance

37. 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.



Immigration Act 2009, s 300 Compliance

38. INZ/MoH Publically Funded Health Eligibility

To enable the Ministry of Health to determine an Individual's:

- eligibility for access to publically funded health and disability support services; or
- liability to pay for publically funded health and disability support services received.

MoH disclosure to INZ: MoH sends names, date of birth and NHI number to INZ for matching.

INZ disclosure to MoH: INZ provides names, gender, birth date, nationality, visa or permit type and start and expiry dates, and dates the person entered or left New Zealand. INZ may also disclose details of a parent or guardian of a young person.



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

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 2018, Schedule 6, cl 13 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 2018, Schedule 6, cl 15 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 Security Act 2018, s 380 and Social Welfare (Reciprocity with Australia) Order 2017 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 Security Act 2018, s 380 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 Security Act 2018, s 380 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.



Social Security Act 2018, s 380 and Social Security (Reciprocity with the United Kingdom) Order 1990 Compliance

46. United Kingdom/MSD Social Welfare Reciprocity

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

UK disclosure to MSD: includes full name, date of birth, marital status, address, entitlement information and Social Security numbers.

MSD disclosure to UK: includes full name, date of birth, marital status, address, entitlement information and New Zealand Client Number.



Tax Administration Act 1994, s 85A (replaced by Schedule 7 Part C subpart 2 cl 43) Compliance

47. 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.



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(s) name(s) Approval Date	Reason	Grounds
Accident Compensation Corporation		
IR/ACC – Compensation & Levies 26 April 2019	Efficiency and security	Timely delivery of data
Department of Internal Affairs		
Births, Deaths, & Marriages, Citizenship, & Passports/ Identity Verification Service – Identity Verification 25 March 2019	Efficiency – transfer is within agency	Timely delivery of data
Immigration NZ/Identity Verification Service – Identity Verification 25 March 2019	Efficiency and security	Timely delivery of data
Inland Revenue		
Customs/IR – Child Support & Student Loans 19 September 2018	Efficiency and security	Timely delivery of data
Births/IR – Newborns Tax Number 19 September 2018	Efficiency and security	Timely delivery of data
Ministry of Justice		
IR/Justice Fines – Defaulters Tracing 29 January 2019	Efficiency and security	Timely delivery of data
Ministry of Social Development		
ACC/MSD – Benefit Eligibility 17 October 2018	Efficiency and security	Timely delivery of data
Customs/MSD – Arrivals and Departures 19 January 2019	Efficiency and security	Satisfactory audit result
Customs/MSD – Periods of Residence 25 March 2019	Efficiency	Satisfactory audit result
MBIE		
NZTA/Registered Motor Vehicle Traders – Motor Vehicle Sellers 30 October 2018	Efficiency and security	Satisfactory audit result
New Zealand Transport Agency		
BDM (Deaths)/NZTA – Deceased Drivers Licence Holders 30 October 2018	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 2019

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 2019, 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 2019; 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; and
- 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 2019, 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; and
 - complies with generally accepted accounting practice in New Zealand.

Our audit was completed on 31 October 2019. 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



Privacy Commissioner
Te Mana Mātāpono Matatapu

Published by the Office of the Privacy Commissioner
PO Box 10094
Wellington
109-111 Featherston Street
Wellington 6143
www.privacy.org.nz

© 2019 The Privacy Commissioner
ISSN 1179-9838 (Print)
ISSN 1179-9846 (Online)