Privacy Commissioner
Te Mana Matapono Matatapu

Briefing for the Incoming Minister of Justice: Hon Andrew Little

Office of the Privacy Commissioner

October 2017

SNAPSHOT

Law reform an urgent priority

- New Zealand's first website was created in 1992, after NZ's privacy law was drafted and introduced to Parliament. In the following quarter of a century New Zealand and the world has become ever more digital and our economy and society has been transformed in the process. In 1996 only one in five New Zealanders had heard of the internet – now New Zealanders' use of the internet is among the highest in the world.[1] Meanwhile, our key information privacy law has remained unchanged.

- The Law Commission comprehensively reviewed the Privacy Act and made more than 100 recommendations for change in 2011. Many of the major proposals were accepted by the previous Government. Drafting of a new Privacy Bill incorporating those recommendations is close to being ready for introduction.

- I proposed additional reforms in December 2016 that respond to the rapid changes that have occurred since the 2011 review.

- New Zealand has a competitive trade advantage from the formal recognition by Europe that our privacy law meets current EU standards to allow the unrestricted transfer of European data for processing. That status is at risk as our law falls behind international standards.

PART 1 – OVERVIEW

1.1. The Office of the Privacy Commissioner (OPC) is an Independent Crown Entity, with business, civil society and government jurisdiction. The Privacy Commissioner is a corporation sole. Comparable privacy and data protection authorities exist in more than 120 nations.

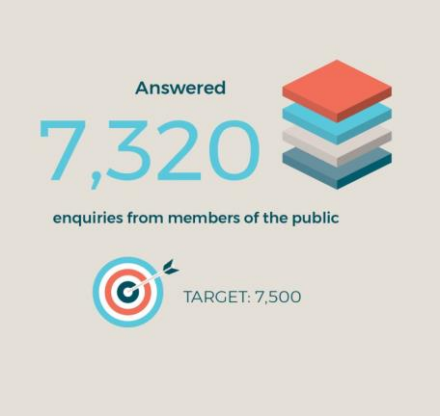
1.2. The Privacy Act was passed by unanimous vote of Parliament in 1993, and has received cross-party support across successive governments.

[1] Source: OECD Digital Economy Outlook 2017

1.3. Information privacy and data protection is a dynamic field that has developed rapidly against a background of technology changes such as cloud computing and data analytics; social networking; cross-border data transfers; the Internet of Things; artificial intelligence and robotics.

1.4. Public awareness and interest has grown over the time since the Office was established in 1993. Our own regular opinion polls, including a UMR survey in 2016, show that New Zealanders are concerned about privacy, especially about whether their personal information is well-managed and protected. Two-thirds (65%) of New Zealanders were concerned about privacy. Nearly half (46%) of all New Zealanders say they have become 'more concerned' about privacy issues over the past few years.

1.5. The operation of an innovative and vigorous economy and an efficient government depends on confidence in organisations' ability to treat personal information appropriately. Companies and government agencies have found that inadequate attention to privacy of customer and client data can erode trust and confidence, impede the delivery of essential public services, and wipe out shareholder value.



1.6. At the June 2016 OECD Ministerial Meeting in Cancun, participating Ministers declared the importance of building and strengthening trust in order to maximise the benefits of the digital economy. The declaration included a commitment to promote a general policy of accountability and transparency. Those Ministers recognised that trust, privacy and transparency are essential elements of civic and digital engagement.

1.7. While the current legal framework has been robust and flexible, there is a pressing need to refresh that framework. The Government has accepted many of the major law reform proposals recommended by the Law Commission's 2011 comprehensive review of privacy. A new Privacy Bill is currently being drafted. Key changes will give the Commissioner greater powers to enforce the Act.

1.8. Aspects of the Law Commission's recommendations to improve information sharing practices were enacted by the Government in 2013. These changes introduced the Approved Information Sharing Agreements (AISA) mechanism in Part 9A of the Privacy Act.

1.9. In 2014, the Government announced a formal response to the Law Commission review and committed to major privacy law reform. The Privacy Commissioner supports those reform proposals. The operating environment continues to develop and law reform is now well overdue. The Commissioner made further significant recommendations for necessary law change in December 2016, which are detailed in paragraph 2.4.

PART 2 – AREAS OF STRATEGIC FOCUS

Privacy law reform – modernising the Act

2.1. There is an urgent need for privacy law reform. All key international instruments on information privacy on which domestic privacy laws are based have been reviewed or updated in the last decade including, most relevantly for NZ, those of the OECD (2013), EU (2016) and APEC (2016). Most existing privacy laws around the world have been reformed in the last 3 years or are currently being reviewed and updated.[2] Internationally, the most influential is the EU General Data Protection Regulation (GDPR) that comes into force in May 2018 and affects Europe and many of our key trading partners. Its standards lift the baseline internationally in response to the challenges to consumers and data protection in today's global digital economy.

2.2. The Law Commission's comprehensive review of privacy in 2011 made numerous recommendations for change to the Privacy Act, to enable the law to better keep pace with the extraordinary changes to information and communications technology that had occurred in the preceding 20 years. The Government accepted the majority of those recommendations and we were pleased to support the Government's reform proposal.

2.3. A new Privacy Bill is being drafted by PCO and we have been closely engaged with officials throughout this process. Key changes include:

- modernising the Privacy Act;
- empowering the Commissioner to issue a compliance notice in the event of a breach of the Act;
- empowering the Commissioner to issue a determination when a person has requested access to personal information under principle 6 and has been refused;
- the introduction of mandatory reporting of serious data breaches, to bring New Zealand into line with international best practice. We currently receive voluntary notifications from agencies in the event of a data breach.

2.4. In 2016, given that five years had elapsed, we initiated a review of the operation of the Privacy Act in accordance with s.26. The report was given to the previous Minister in December 2016 and was presented to the House in January 2017. We recommended that, in addition to the reforms announced in 2014, Government should consider:

- empowering the Privacy Commissioner to apply to the High Court for a civil penalty to be imposed in cases of serious breaches (up to $100,000 in the case of an individual and up to $1 million in the case of a body corporate);

[2] Source: ICDPPC Census 2017

- protection against the risk that individuals can be unexpectedly identified from data that had been purportedly anonymised;
- introducing data portability as a consumer right;
- a power to require an agency to demonstrate its ongoing compliance with the Act;
- narrowing the defences available to agencies that obstruct the Privacy Commissioner or fail to comply with a lawful requirement of the Commissioner; and
- reforming the public register principles in the Act and providing for the suppression of personal information in public registers where there is a safety risk.

2.5. We continue to support the Law Commission recommendation to bring the Office of the Director of Human Rights Proceedings into this Office, despite the 2014 Cabinet decision not to accept the recommendation. We ask that the new Government reconsiders this matter alone amongst the reform proposals. There are significant efficiencies to be gained by a streamlined process, which would also bring a swifter resolution for the parties. In the current model, the Director effectively re-examines the case before bringing proceedings in the Tribunal. In those instances where the Director decides not to intervene, complainants are then faced with initiating proceedings themselves after a period of delay.

Information Sharing

2.6. Improving the public sector's use of personal information to support the delivery of better public services has been a government priority.

2.7. A number of mechanisms in the Privacy Act allow information sharing to occur. These include the exceptions to the privacy principles; the ability for the Privacy Commissioner to issue Codes (Part 6); the information matching regime set out in Part 10; and the provision for Approved Information Sharing Agreements (AISAs) contained in Part 9A, which was added in 2013. There is further provision to share law enforcement information in Part 11 and Schedule 5.

2.8. The Act has ample scope for the sharing of government-held information and my Office has worked closely with agencies to identify and understand any unintended impediments to progressing initiatives requiring information sharing.

2.9. A Cabinet Directive in 2016 instructed agencies to identify any barriers to information sharing proposals. We put significant effort into supporting agencies to find privacy-protective ways to share information and resolve specific implementation issues.

2.10. The feedback from agencies was overwhelmingly that the barriers to information sharing were operational. These included issues such as a lack of interoperability between IT systems, security concerns, cost, and differing priorities between agencies.

2.11. OPC has a statutory monitoring role in the development of AISAs. This is an independent role and we cannot actively promote or steer the direction of particular AISAs. We have published guidance and a training module on AISAs to assist agencies. Currently, there are seven AISAs.

2.12. On a day-to-day level we continue to work with agencies in developing AISAs. Our observation is that the number of AISAs either finalised or in development is reaching the point where agencies are now able to borrow from the approach taken by others.

Additional efforts to support information sharing initiatives

2.13. It has become evident that many of the perceived barriers to information sharing are based in misunderstanding or uncertainty of the law. We have responded to the need for clear legal guidance for agencies and have developed two new mechanisms to meet this demand:

- Advisory opinions
- OPC's Trusted Sharing Consultancy Service.

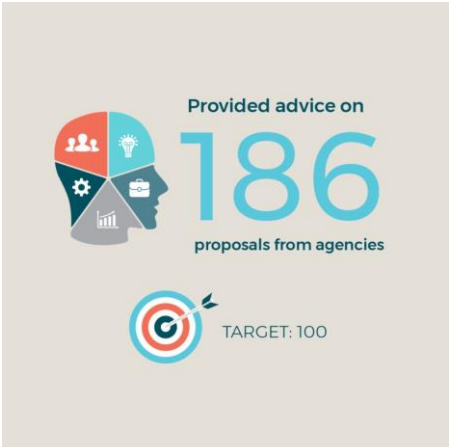
The ongoing demand for and success of the Consultancy Service illustrates that the current legislative environment does not inhibit information sharing. None of the agencies spoken to identified the Privacy Act as the obstacle to progressing information sharing work.

2.14. The Government Chief Privacy Officer (GCPO) and Government Chief Information Officer (GCIO) within DIA also contribute to the wider aim of supporting and developing privacy maturity and information sharing initiatives across the public sector.

Policy

2.15. The Privacy Commissioner gives independent advice to select committees, Ministers, and their departments on policy and legislative proposals. For instance, the Privacy Commissioner was consulted in the development of policy leading to the Intelligence and Security Act 2017. The law changes took effect in late September and mean the intelligence and security agencies are now subject to many of the Privacy Act principles.

2.16. In April 2017, we released an inquiry report into the collection of individual client-level data by MSD, in response to direct concerns raised with us by social sector NGOs. The practice, which required further refinement, was subsequently put on hold. My Office is well placed to contribute early in the development of such proposals to ensure privacy considerations are adequately factored into the design.



PART 3 – MODERNISING OUR OPERATION

Examples of recent initiatives

3.1. **Priv-o-Matic**
Our online privacy statement generator for small business won the People's Choice Award in the NZ Open Source Awards 2016.

3.2. **AskUs**
Our interactive online FAQ tool provides the answer to any privacy question. We are actively developing this resource in response to questions posed by the public. Uptake has exceeded expectations: 8,433 questions answered.

3.3. **Inquiry report into client level data collection**
In April 2017, we released an inquiry into the collection of individual client-level data by MSD and in response to concerns raised with us by NGOs. The practice, which required further refinement, was subsequently put on hold.

3.4. **Network of intelligence and security oversight agencies**
We established a NZ oversight group of authorities and, in conjunction with IGIS, are seeking to establish an informal network of agencies in Five Eyes jurisdictions.

3.5. **111 caller location**
An amendment to the Telecommunications Information Privacy Code enabling the use of 111 caller location to provide faster response by emergency teams has been noted internationally as a feature of a successful implementation of this technology in a trusted environment.

3.6. **Regional Outreach**
An ongoing programme of community outreach in geographically diverse regions throughout New Zealand.

Outreach and public facing work

3.7. Our website (www.privacy.org.nz) is our primary means of communicating our work. We actively engage with stakeholders through online channels such as our blog, Twitter, YouTube and Facebook.

3.8. We have a fortnightly e-newsletter: *PrivacyNews*

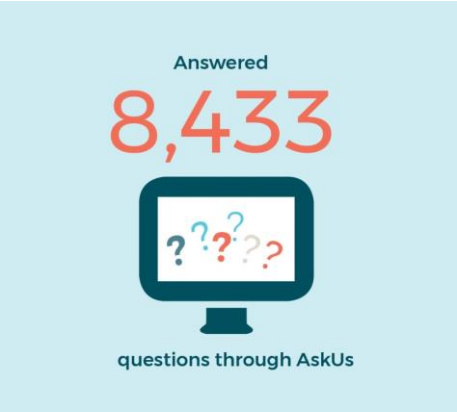
3.9. We provide presentations at many events and host our own events, such as Privacy Forums and PrivacyLive, which we often livestream to make them more widely available.

3.10. We are active in responding to media and have cooperative and positive engagement.

3.11. We run a full public speaking programme across a range of industry sectors, including health, technology and legal, and wider civil society groups.

3.12. We aim to provide well-targeted guidance and resources that are easily accessible. We have developed a number of online tools to support this, including:

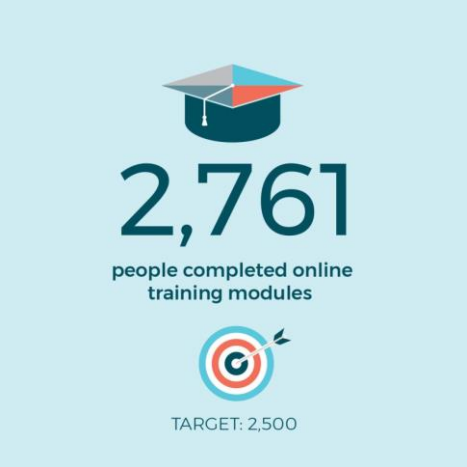
- Priv-o-Matic: a five-minute online privacy statement generator for small business.
- *AskUs:* an interactive online FAQ tool that provides the answer to any privacy question. We are actively developing this resource in response to questions posed by the public. It is a significant supplement to our public-facing work.
- *AboutMe:* an online tool to make it simple for people to lodge information access requests.



- Privacy Directory - our online directory of privacy professionals to help develop a community of expertise.
- Secure online complaint lodgement through our website.

Education & Training

3.13. We have invested in the development of a suite of e-learning modules. The uptake for these has been encouraging, with 2,700 people completing modules in the last year. Online delivery enables us to provide privacy training across the country, regardless of geographic location.



3.14. There are currently seven modules, including employment and privacy; health, and credit reporting. Further modules are being developed for government policy advisers, and a health privacy primer.

3.15. The modules are accessible on our website and are free. This means we are reaching audiences that would have been impossible with face-to-face training. We are responding to user feedback and increasingly producing short, scenario-driven modules, such as PrivacyABC, which can be completed in 30 minutes.

Regional Outreach

4.1 We have an ongoing programme of regional outreach visits to engage directly with stakeholder groups across the country. These seek to improve access to our services and raise awareness of the law. Our online tools assist our outreach efforts to all New Zealanders.

Working in partnership: Oversight of Intelligence & Security matters

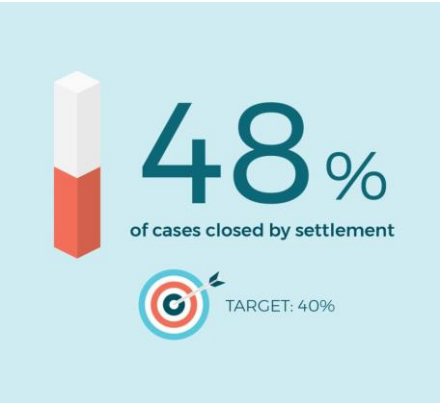
4.2 The Privacy Commissioner, in conjunction with the IGIS, is seeking to establish an informal network of intelligence and security oversight agencies in the Five Eyes jurisdictions. Within New Zealand, there has been an oversight group established that includes the IGIS, Privacy Commissioner, Auditor-General, and the Chief Ombudsman.

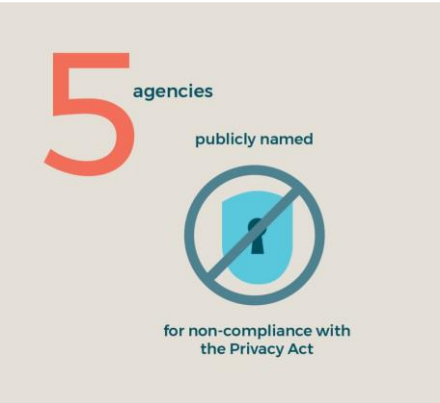
Dispute resolution and enhanced enforcement processes

4.3 We aim to have a high quality dispute resolution process that is as effective and swift as possible. We seek to make it easy for parties to resolve differences, and we are focused upon using the full range of tools available to achieve this including, for instance, bringing parties together in compulsory conferences to enable a rapid resolution wherever possible.

4.4 We work closely with other key regulators to resolve complaints from the public. In the case of the Ombudsman our jurisdictions are complementary. We similarly liaise with industry complaint bodies, such as the BSA, Press Council, Banking Ombudsman, etc.

4.5 We have a 'naming policy' that outlines the approach we take in publicly naming an agency that breaches the law. This has been employed to good effect on five occasions since it has taken effect.





Litigation

4.6 The Human Rights Review Tribunal has exclusive jurisdiction for the delivery of remedies and rulings in privacy complaints. It has become apparent over time that there are structural and resourcing difficulties in the current configuration of the Tribunal. The jurisdiction is relatively broad and the Chair is required by statute to sit in on every hearing.

4.7 The combined effect is that there are significant delays in cases being decided and the effectiveness of the Tribunal as a means of dispute resolution is greatly reduced. The impact of this upon parties' ability to have access to justice is concerning. We understand the Tribunal has, amongst other measures, taken drastic action by suspending the setting down of cases for hearing unless urgent, to address the significant backlog.

4.8 We would welcome the opportunity to work with the Tribunal and Ministry to develop proposals to address what has become a pressing problem in the administration of justice in this area.

International

4.9 The Office of the Privacy Commissioner participates in a number of key international networks. The principal forums to meet with our peer authorities are at regional level the Asia Pacific Privacy Authorities (APPA), and at global level the International Conference of Data Protection and Privacy Commissioners (ICDPPC).

4.10 The New Zealand Commissioner has just completed a three year term as Chair of this key international conference, which also brought with it the duty to provide an international secretariat. As Chair and Secretariat, a special emphasis was placed upon upgrading the network's capacity for working more strategically and effectively.

4.11 OPC contributes to the work of specialised peer networks such as the APEC Cross-border Privacy Enforcement Network (CPEA), Global Privacy Enforcement Network (GPEN) and the International Working Group on Data Protection in Telecommunications (the Berlin Group).

4.12 In addition the Office provides a NZ delegate in an expert capacity to the relevant committees of two international governmental organisations.[3]

New Zealand's EU Adequacy finding

4.13 The European Commission decided in December 2012 that New Zealand law provides an 'adequate level of data protection' for the purposes of existing EU law. A finding of 'adequacy' denotes that New Zealand is deemed to have sufficient data protection regulation in place to meet EU legal requirements for the transfer of European-originated personal data for processing. The effect is to enhance trade opportunities by allowing European business to transfer data to New Zealand for processing.

[3] APEC's Electronic Commerce Steering Group Data Privacy Subgroup (ECSG DPS), and the OECD Working Party on Security and Privacy in the Digital Economy (SPDE).

4.14 The EU law will be replaced by the General Data Protection Regulation (GDPR) that takes effect in May 2018. The effect of this law change may bring New Zealand's adequacy status into question, unless New Zealand law is modernised to the EU 'gold standard' of the GDPR or Council of Europe Convention 108. New Zealand's once favourable position internationally is now relatively poor due to our outdated law. We are in regular communication with the European Commission on this point.

Sectoral codes of practice

4.15 The Privacy Commissioner can independently issue statutory codes to regulate personal information handling.

4.16 Major sectoral codes regulate the health sector, telecommunications sector, and credit reporters.

4.17 The Telecommunications Information Privacy Code was amended in January 2017 to allow for non-consensual automated release of mobile phone location to assist emergency teams in responding to 111 calls. Recent amendments include consequential changes to several codes to reflect the Privacy Act amendments from the Intelligence and Security Act 2017.

4.18 Codes can be used to adapt the law to specific circumstances. For instance, in response to industry requests, OPC amended the credit reporting code to introduce a more comprehensive credit reporting regime for New Zealand to support a more responsible lending environment.

Privacy Commissioner
Te Mana Matapono Matatapu

Privacy Commissioner **Term Commenced**	John Edwards February 2014
Legal Entity	Corporation Sole (Privacy Act 1993) Independent Crown Entity (Crown Entities Act 2004)
No. of Staff	36.8 FTEs
Office Locations	Wellington (24.9 FTEs) Auckland (11.9 FTEs)
Budget	$4.970m (2017/18)
No. of Enquiries and Complaints received	Public enquiries 8,000 per annum Complaints 800 per annum Media enquiries 250 per annum
Privacy Bill	A new Privacy Bill is being drafted to replace the Privacy Act which has been in force for over 20 years. The Bill provides new enforcement powers for the Commissioner.

Funding

- OPC received an increase to baseline funding in the 2014 budget from $3.58m in 2013/2014 to $4.97m in the out-years (plus an additional $0.201m for 2014/15). The increased baseline reflects the increased demands for the Privacy Commissioner to be an active participant in the provision of Better Public Services and information sharing across government.

- The law reforms will have further implications for our workload and resourcing. There is designated additional contingency funding, allocated as part of Budget 2014 in response to the proposed 2014 Privacy Act reforms. This funding currently sits with Treasury until Cabinet approves the release of the funds.

Privacy Commissioner as independent regulator and watchdog

The functions of the Commissioner are set out in s.13 of the Privacy Act, and include:

- advising on the risks and benefits of new technologies, policy proposals or initiatives
- commenting on proposed legislation (LAC Guidelines also promote consistency with the Privacy Act and principles)
- overseeing authorised government data matching programmes
- monitoring the development of Authorised Information Sharing Agreements (AISAs)
- promoting public understanding of privacy and personal information protection issues
- investigating complaints from the public about breaches of privacy in private and public sectors
- issuing codes of practice to protect the public.