Privacy Commissioner
Te Mana Matapono Matatapu

Briefing for the Incoming Minister of Justice

Office of the Privacy Commissioner

October 2014

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	33 FTEs
Office Locations	Wellington (21.4 FTEs) Auckland (11.6 FTEs)
Budget	$5.171m (2014/15)
No. of Enquiries and Complaints received	Public Enquiries 9,000 per annum Complaints 800 per annum Media Enquiries 300 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.

PART 1 – EXECUTIVE SUMMARY

1.1 In recent years, privacy has emerged as a prominent subject of public debate and discussion both domestically and internationally. Government agencies and corporations have both found that inadequate attention to privacy law and privacy values can erode trust and confidence, impede the delivery of public services, and wipe out shareholder value.

1.2 Our own research, including a UMR survey conducted at the beginning of this year, shows that New Zealanders are more concerned about privacy, especially about whether their personal information is well managed and protected. The survey showed that half of all New Zealanders say they have become 'more concerned' about privacy issues over the past few years. This is a continuation of a trend, and shows the highest level of public concern since the survey began in 2001.

1.3 Trust and confidence in organisations' ability to treat personal information appropriately is a condition precedent to economic activity and the efficient delivery of public services. A well functioning regulatory body is a necessary component in the maintenance of trust and confidence.

1.4 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 and administers the Privacy Act. Comparable privacy and data protection authorities exist in most developed nations.

1.5 Information privacy and data protection is a dynamic field that has developed rapidly against a background of technology changes such as cloud computing; social networking; cross-border data transfers; biometrics; data sharing; online fraud and security.

1.6 The operating environment for OPC has also undergone substantial change. Notably, there has been a change of leadership in recent months. John Edwards took up office in February 2014. Mr Edwards has a background as a barrister and information law specialist.

1.7 While the current legal framework has proved to be robust, there is a clear need to refresh that framework to better suit the current environment. The Government has accepted the major law reform proposals recommended by the Law Commission's comprehensive review of privacy. A new Privacy Bill is currently being drafted and key changes will give the Commissioner greater powers to enforce the Act. We are hopeful that this work will be a high priority in the Government's legislation programme.

1.8 The 2014 budget provided much needed additional targeted funding for OPC through Vote Justice. This increase to baseline funding reflects changing demands upon the Office over a number of years and the fact that good information privacy practice is integral to the success of Better Public Services, especially Key Result Areas 4, 9 and 10.

1.9 The establishment of the new role of Government Chief Privacy Officer (GCPO) is a positive development that supports and enhances the regulatory and watchdog functions of OPC. It reflects an evolving understanding across government of the fact that personal data and information are strategic assets held by government as a steward on behalf of the New Zealand public. We are applying considerable effort and resource to support that role and to minimise role confusion and duplication.

1.10 Other areas of priority are to:

- build capacity in the market for privacy expertise
- support Better Public Services initiatives

- develop comprehensive and clear guidance to help businesses and individuals comply with the law and prepare for law changes
- continue to collaborate with international colleagues to achieve effective enforcement outcomes
- monitor and develop guidance on Authorised Information Sharing Agreements (AISAs)
- work with the Vulnerable Children's Board, Child Protection Teams and the Children's Commissioner and others to resolve information sharing dilemmas arising in the context of care plans for vulnerable children
- develop our public outreach programme through redeveloping our website and online resources, and targeting areas of identified need
- enhance our enforcement and dispute resolution processes, for instance by:
  - greater use of powers such as compulsory conferences
  - introduction of clear policy around naming agencies
  - maintaining a strong resolution focus

PART 2 – WHO WE ARE

Role of Privacy Commissioner as independent regulator and watchdog

2.1 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
- 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 both private and public sectors
- issuing codes of practice for industry.

2.2 OPC received an increase to baseline funding in the 2014 budget from $3.58m in 2013/2014 to $4.97m in out years (plus an additional $0.201m for 2014/15).

2.3 The increased baseline reflects the expectations placed on my office to meet the increased demands for the Privacy Commissioner to be an active participant in the provision of Better Public Services and information sharing across government.

2.4 The law reforms will have implications for our workload and resourcing. We will be able to provide further detail arising from the law reforms and the implications for OPC in due course.

Current work plan - Project focus

2.5 Much of our work is prescribed in statute, or is demand driven, such as contributions to government policy initiatives. However we are increasingly moving to project based work and are applying new resources and discretionary capacity to projects that support goals identified in our Statement of Intent. Current projects include:

- **Privacy Impact Assessment**: updating comprehensive guidance for business and government agencies
- **Online training materials**: developing online training modules for effective and easy to access privacy education and training
- **Technology strategy**: working with industry stakeholders to develop priority areas of focus for OPC
- **Vulnerable Children**: developing effective information sharing guidance to assist multi-agency Children's Action Teams
- **Security and Intelligence**: working with the Inspector General of Intelligence and Security, The Chief Ombudsman, and Auditor-General to provide robust and coordinated oversight of security and intelligence agencies
- **Approved Information Sharing Agreements:** these were a key initiative enacted by Government in February 2013 to allow for better coordination between agencies to deliver public services. They have the potential to reduce uncertainty and provide safeguards but as yet have been under-utilised. We are working with agencies on specific projects, and will be providing further generic guidance for public servants on using this tool.

Administration

2.6 We have reviewed our governance processes to ensure they reflect best practice for an independent Crown entity and corporation sole. This review began with a stocktake of current arrangements commissioned in February 2014. All the recommendations of that review have now been implemented, including establishing a governance advisory body with external expert advisers. These initiatives have been welcomed by control and monitoring agencies such as the Office of the Auditor-General and the Ministry of Justice.

PART 3 – LOOKING FORWARD

Privacy law reform - nature of changes

3.1 The Privacy Act was passed by unanimous vote of Parliament in 1993. Key issues at the time were to meet OECD Guidelines Governing the Protection of Privacy and Trans-border Flows of Personal Data to protect our international trade; and to allow the government to match databases to detect fraud (eg benefits and employment) while monitoring and providing reassurance to the public in general.

3.2 The free-flow of data across borders persists as a signature issue for data protection authorities. International standards and cross-border enforcement are an increasingly important dimension to effective privacy and data protection. New Zealand's Privacy Act has been described as "technology neutral" and this feature has enabled it to continue to generally function well over two decades. In 2012, New Zealand law was found to meet EU standards, enabling the transfer of personal data to NZ for processing.

3.3 The Law Commission's comprehensive review of privacy made numerous recommendations for change to the 20 year old Privacy Act, to enable the law to better keep pace with the extraordinary changes to information and communications technology that had occurred. The Government has accepted the majority of those recommendations.

3.4 A new Privacy Bill is currently being drafted by PCO and we are working closely with officials throughout this process. Key changes will include:

- 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.)

3.5 We were pleased to support the Government's reform proposal and in February the incoming Commissioner endorsed the Office's support for the proposed amendments, with two reservations. The Government has not accepted two recommendations of the Law Commission which we consider would significantly enhance the efficacy of the Office, and the administration of justice in this area. These are:

- That the functions of the Director of Human Rights Proceedings should be brought within the Office of the Privacy Commissioner.
- That the Privacy Commissioner should have some statutory ability to require an agency to view information systems *in situ* rather than just an ability to require the production of information.

Government Chief Privacy Officer

3.6 The role of Government Chief Privacy Officer (GCPO) was established early in 2014 within DIA. We are working closely with the GCPO in furthering our complementary roles. The GCPO's focus is on lifting privacy and information management standards across government. The Privacy Commissioner's combined private and public sector jurisdiction; watchdog and regulatory role operate in parallel to the GCPO. We anticipate positive combined outcomes as we work together going forward.

Outreach and public facing work

3.7 Our website (www.privacy.org.nz) has become our primary means of communicating our work. We are seeking to do more to engage and interact online through our website and by using our blog, Twitter, YouTube and Facebook channels.

3.8 Our aim is to provide well-targeted guidance and resources in easily accessible ways. We will be enabling privacy complaints to be lodged online to make it easier to access our dispute resolution processes. We are starting a directory of privacy professionals on our website to help develop a community of expertise. We are in the early stages of developing an accreditation process.

3.9 We are working to target outreach to areas of identified need. Together with Netsafe and with the support of UNESCO, we developed a teaching resource for primary and intermediate schools to help children to learn to be safe online.

3.10 We are developing a programme of regional outreach visits and clinics to better respond to information management and privacy needs across the country. We are active in responding to media and in participating in public speaking engagements to a range of groups.

Dispute resolution and enhanced enforcement processes

3.11 We aim to have a complaints investigation process that is as effective as it can be in obtaining resolutions for people. We seek to make it easy for parties to a dispute to resolve differences, and we are focused upon using the full range of tools available to achieve this.

3.12 Experience over the years has demonstrated that there are instances when we need to make better use of our statutory enforcement powers. For instance, we

will be bringing parties together in compulsory conferences to enable a swift resolution wherever possible.

3.13 We recently released a 'naming policy' that outlines the approach we plan to take in more often publicly naming an agency that breaches the law.

Litigation

3.14 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.

3.15 The jurisdiction is relatively broad, covering three jurisdictions (including Part 1A of NZ Bill of Rights Act; Human Rights Act; Health & Disability Commissioner Act; as well as the Privacy Act). The Chair is required by statute to sit in on every hearing although his role is limited to part-time (0.6 time).

3.16 The administrative support for the Chair is provided by his own legal practice. The Chair runs the pre-trial teleconferences and prepares the minutes for those; he writes all the decisions.

3.17 The combined effect is that there are significant delays in cases being brought before the HRRT 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.

3.18 This problem will be exacerbated by the increased workload that will be funnelled through the Tribunal as a result of the law reform changes (particularly in challenges to access determinations and compliance notices) and must be urgently addressed.

3.19 We would be happy to work with the Tribunal and Ministry to develop proposals for addressing what has become a very pressing problem in the administration of justice in this area.

International

3.20 There is an underlying international dimension to many aspects of information privacy. Most significant is the cross-border transfer of personal information that is now an ordinary daily feature of business and personal life.

3.21 Global privacy enforcement authorities need to cooperate across borders to protect against privacy threats. We engage with overseas counterparts in a number of ways to enhance problem solving, policy solutions and provide more effective regulation. For example:

- international collaboration to develop common standards to facilitate business transactions across borders in ways that protect the interests of individuals;
- international cooperation to effectively enforce a privacy or security breach, for instance where a company's actions affect the citizens in another country;
- 'advance warnings' and insights from other countries as they encounter privacy challenges.

3.22 The principal international forums are:

- Asia Pacific Privacy Authorities (APPA)
- APEC
- OECD
- Global Privacy Enforcement Network (GPEN)
- International Conference of Data Protection and Privacy Commissioners.

3.23 The European Commission decided in December 2012 that New Zealand's law provides an 'adequate level of data protection' for the purposes of existing EU law. This enhances trade opportunities by allowing European business to transfer data to New Zealand for processing. The EU law is now under review and due to be replaced by new regulations. We are working to ensure that European officials understand the need for a smooth transition of these adequacy decisions into any new regime.

Industry codes of practice

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

3.25 Major industry codes include the Health Information Privacy Code, the Telecommunications Information Privacy Code, and the Credit Reporting Privacy Code.

3.26 Codes can be useful in adapting 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. These developments were aimed at supporting a more responsible lending environment. Major credit reporters and lenders recognise that there is an urgent need for public education about the credit reporting system and particularly the new monthly repayment recording that will affect almost all adult New Zealanders.

3.27 Recently, the credit code was amended to limit the amount credit reporters can charge when providing urgent credit reports to individuals.

Policy

3.28 OPC gives independent advice to Ministers, their departments and select committees on policy and legislative proposals.

3.29 The Ministry of Health provides funding towards a position within OPC to respond to the wide-ranging privacy issues arising in the health sector, such as in the development of electronic shared care records. We have completed a review of three regional e-record programmes and a report of that is publicly available.

3.30 OPC has a statutory monitoring role in the development of Authorised Information Sharing Agreements (AISAs) between agencies. The implementation of the new AISA regime has been slower than expected and agencies have experienced some difficulties. OPC has an independent role and cannot actively promote or steer the direction of particular AISAs. We will publish guidance, but there is a risk that the tool provided by government will be seen to be too hard and will not be used. Of the 34 agreements we were told were coming, only two have been issued, and we are aware of work on one other.