Australian Government

Office of the Privacy Commissioner

Privacy Commissioner

Te Mana Matapono Matatapu

MEMORANDUM OF UNDERSTANDING

BETWEEN

THE OFFICE OF THE AUSTRALIAN PRIVACY COMMISSIONER

AND

THE OFFICE OF THE NEW ZEALAND PRIVACY COMMISSIONER

Memorandum of Understanding between the Office of the Australian Privacy Commissioner and the Office of the New Zealand Privacy Commissioner

1. Participants

1.1 This Memorandum of Understanding (**MOU**) is between:

a. the Office of the Australian Privacy Commissioner (**APC**) and

b. the Office of the New Zealand Privacy Commissioner (**NZPC**)

referred to as **the participants**.

1.2 APC is an independent statutory office established by the Privacy Act 1988 enacted by the Parliament of Australia (the **Australian Privacy Act**) to perform functions vested in the office by that Act and other legislation. APC consists of the Privacy Commissioner and the staff of the office.

1.3 NZPC is an independent Crown entity established by the Privacy Act 1993 enacted by the Parliament of New Zealand (the **New Zealand Privacy Act**) to perform functions vested in the office by that Act and other legislation. NZPC consists of the Privacy Commissioner and the staff of the office.

2. Purpose

2.1 APC and NZPC enter into this MOU to:

- enhance the exchange of information and cooperation between the participants
- promote cross-border cooperation in investigation and enforcement
- assist each other in training, education, promotion, policy and compliance activity
- provide a practical means to meet cooperative aspirations set out in the APEC Privacy Framework
- contribute to the objectives of the OECD Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy.

3. Status

3.1 This MOU is not intended to impose legally binding obligations on the participants or affect existing obligations under international law, or create obligations under the laws of the participants.

3.2 The Annexes and Schedules to the MOU do not form part of the MOU, and are included for reference only.

4. Term

4.1 This MOU will come into effect on the date of signature by both participants and will operate for two years.

4.2 Either participant may bring this MOU to an end by giving notice to the other.

4.3 This MOU may be extended if the participants mutually decide.

5. International setting

5.1 Australia and New Zealand are members of the Organisation of Economic Cooperation and Development (OECD). The Australian and New Zealand Privacy Acts are measures to give effect to the OECD Guidelines Governing the Protection of Privacy and Transborder of Flows of Personal Data, 1980. Australia and New Zealand are also members of the Asia Pacific Economic Cooperation which adopted the APEC Privacy Framework in 2005. APC and NZPC are both accredited to the International Conference of Privacy and Data Protection Authorities and to the Asia Pacific Privacy Authorities (**APPA**) forum.

5.2 This MOU accords with the OECD Guidelines, including that member countries should establish procedures to facilitate information exchange related to those guidelines and mutual assistance in the procedural and investigative matters involved. The MOU replaces an MOU earlier entered into in 2006.

5.3 This MOU also responds to further calls at international level for increased information sharing and cooperation between privacy enforcement authorities. Reference is particularly made to:

- the encouragement in the APEC Privacy Framework for member economies to exchange information on privacy protection and to develop cooperative arrangements in privacy investigation and enforcement (see Appendix 1)
- the declaration adopted at the 27th International Conference of Data Protection and Privacy Commissioners to intensify exchange of information and coordination of data protection supervisory activities (see Appendix 2)
- the resolution of the Asia Pacific Privacy Authorities to enhance the current arrangements for the sharing of knowledge and resources between privacy authorities within the region (see Appendix 3)
- the OECD Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy (see Appendix 4).

6. APPA Forum

6.1 APC and NZPC enjoy good existing relationships through the multilateral APPA Forum that currently meets twice each year. This MOU seeks to build on and supplement those existing arrangements and not replace or duplicate them.

7 Liaison

7.1 The participants will convene regular bilateral liaison meetings via video or teleconferencing involving senior management. The purpose of such meetings will be to further the objectives of this MOU at the strategic level. Initially the meetings will be held twice a year at approximate halfway between the dates of APPA forum meetings.

7.2 The first bilateral liaison meeting is to be arranged for February 2009. The contact persons responsible for substantive liaison matters (as set out in Schedules 1 and 2) will schedule the meeting and settle the agenda.

7.3 In addition, the participants will encourage specialist staff in counterpart positions to institute regular or ad hoc teleconferences or video-conferences to share information and experience in their subject areas. The scheduling and organisation of such meetings is to be arranged between the staff concerned.

8. Information Sharing

8.1 The participants undertake to share information about common issues, important and significant privacy events, emerging and evolving issues, and experience of and approaches to policy, compliance and promotional activities. In particular the participants will share information on:

- public attitude research
- privacy research projects
- promotional, education and training programmes and approaches
- trends, techniques and results of enforcement efforts
- audits, inspections and privacy impact assessments
- potential for parallel or joint investigations or enforcement actions
- significant privacy policy issues
- information security problems and approaches
- notable law reform developments
- regulatory experience and developments.

8.2 Each participant intends, where feasible and appropriate, to give the other advance notice of important developments that may have implications for the other party.

8.3 To facilitate cooperation and efficient information sharing, the participants undertake to keep each informed of up to date organisational structures and appropriate contact points within APC and NZPC. With respect to each participant, Schedules 1 and 2 set out:

- organisational charts, and
- lists of appropriate contact points

as at the date of entering into this MOU. The participants will exchange updated Scheduled information on a quarterly basis.

It is intended that this material could also be used for informal contact between APC and NZPC as and when issues present themselves.

9 Cross-border cooperation in investigation and enforcement

9.1 Within the constraints of the Australian and New Zealand Privacy Acts, the participants intend to cooperate in relation to complaints or investigations that may affect the other participant or have a cross-border element.

9.2 As a precursor to any transfer of a complaint, or request for cooperation in an investigation, the participants will consult each other. This will typically involve discussions in general terms between the nominated liaison persons to identify if the other party will have jurisdiction in respect of a complaint or investigation of the type at issue.

9.3 The participants intend generally to share information about the range of matters set out in 8.1, but particularly on their experience in complaint handling, audits and investigations and the potential to undertake joint investigations or enforcement actions.

9.4 The participants intend to explore the usefulness of developing more detailed protocols for handling complaints that may affect the other participant or that have a cross-border element when the first such a complaint occurs.

9.5 In the context of clause 9.4, the participants will also assess the possibility of entering into a complementary bilateral MOU based upon the draft APEC Cooperation Arrangement for Cross-border Privacy Enforcement, currently being prepared for the APEC Privacy Pathfinder. The objective of this would be to pilot that complementary MOU for a limited time and to use that experience to further inform both the APEC Pathfinder and the next review of this MOU.

10. Audit and privacy impact assessment

10.1 The participants intend to share experiences in relation to various techniques designed to investigate and promote compliance with privacy principles including, for example, external audit, self-audit and privacy impact assessment.

11. No obligation to meet requests

11.1 This MOU is to be construed consistently with the right of either participant to decline or limit cooperation on particular investigations, audits or other matters, on the ground that compliance or a request for cooperation will be inconsistent with domestic laws, policies or priorities, or on the ground of resource constraints or based on the absence of mutual interest in the investigations in question.

12. Opportunities for staff transfers, training, exchanges and secondments

12.1 The participants will inform each other of senior or specialised employment vacancies that arise. Wherever possible, such notification will be through APPA channels (currently using the *APPA Alert* bulletin) so as to achieve wider regional benefits.

12.2 The participants intend to further explore opportunities for facilitating arrangements for secondments between the participants. The participants are committed to supporting and utilising the (currently draft) APPA Secondment Framework but do not exclude the possibility of also exploring secondments on a bilateral basis.

12.3 Each participant will endeavour, where appropriate, to consider the feasibility of providing opportunities for staff of the other participant to:

- participate in training programmes it is conducting
- present training programmes for the staff of the other agency
- participate in staff exchanges
- share specialist training resources.

Such initiatives may sometimes be coordinated through the APPA Forum.

13. Costs

13.1 Each agency will bear its own costs of providing information or assistance in accordance with this MOU.

13.2 If the costs of responding to any specific request for assistance, or offer of training or other cooperation are substantial, the agencies may negotiate to share or transfer the costs.

14. Confidentiality

14.1 Information provided in accordance with this MOU will only be used or disclosed for the purposes for which it was provided unless authorised by the participant first providing it.

15. Disputes

15.1 Where there is a dispute between the participants in relation to this MOU, the participants will seek to resolve the issue by negotiation between the persons shown in Schedules 1 and 2 as the principal persons for substantive matters or, failing that, between the respective commissioners.

16. Review of this MOU

16.1 This MOU may be amended at any time by mutual arrangement.

16.2 After this MOU has been in effect for 18 months, the participants will each nominate a representative to jointly review the MOU and its operation and consider whether its amendment or continuation is appropriate.

Dated this 28th day of August 2008

Karen Curtis
Australian Privacy Commissioner

Marie Shroff
New Zealand Privacy Commissioner

Schedule 1

Office of the Australian Privacy Commissioner:
Contacts and organisational plan (as at September 2008)

Part A: Contact details

Physical and postal addresses:

Sydney (head office)	**Canberra**
Office of the Privacy Commissioner PO Box 5218 Sydney NSW 2001 Australia	Office of the Privacy Commissioner PO Box 2999 Canberra City ACT 2601 Australia
Level 8, Piccadilly Tower, 133 Castlereagh Street Sydney NSW 2000	1st floor, AMP Tower 1 Hobart Place Canberra City ACT 2601
Tel +61 2 9284 9800 Fax +61 2 9284 9666	Tel +61 2 6247 3658 Fax +61 2 6247 3358

Principal liaison person for substantive matters: Timothy Pilgrim

Principal liaison person for administrative matters: Timothy Pilgrim

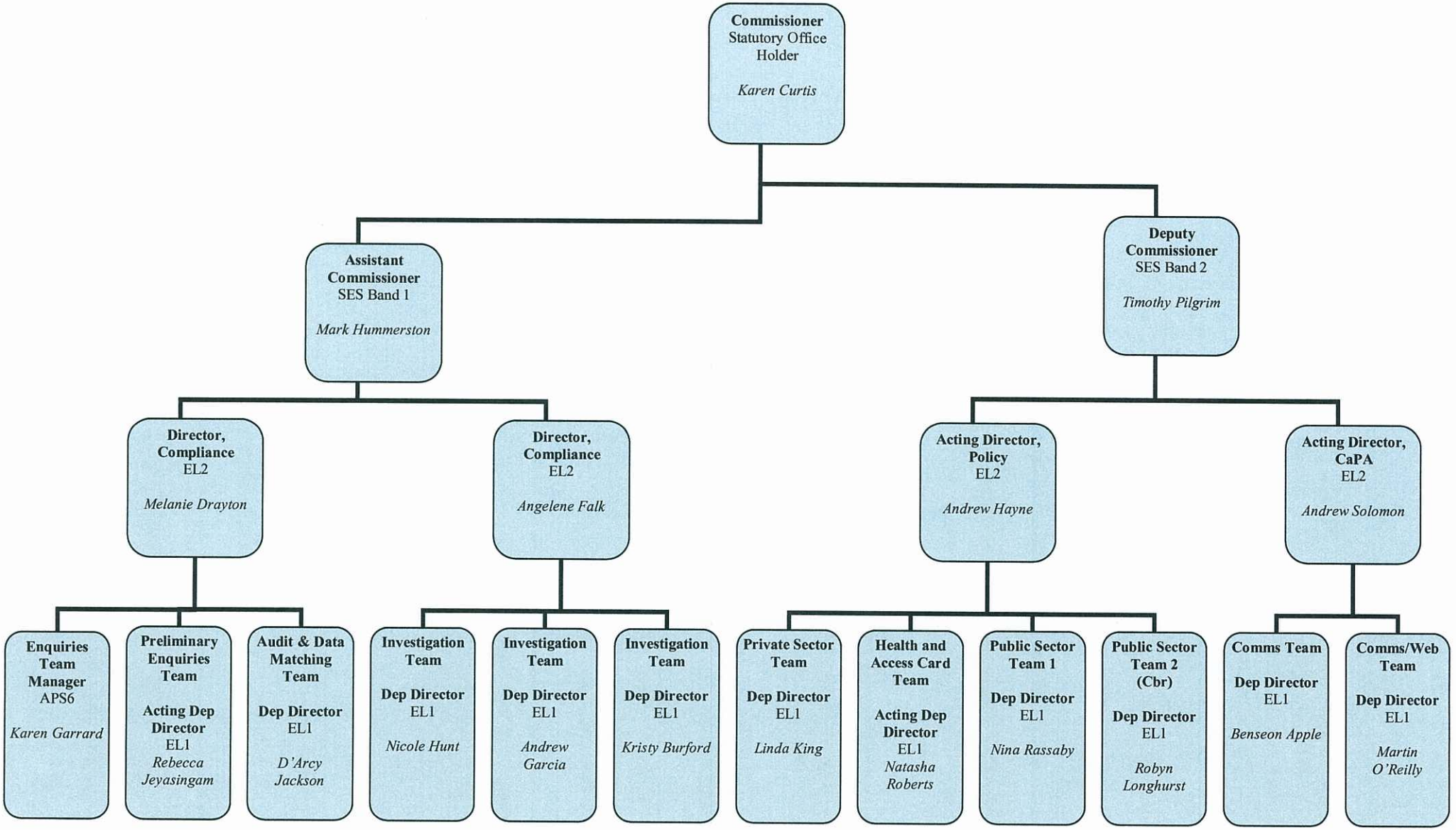
Specialist liaison persons:

Codes of practice:	Andrew Hayne
Complaints:	Mark Hummerston
Corporate services:	Timothy Pilgrim
Data matching:	Mark Hummerston
Legislative issues:	Timothy Pilgrim
Library:	Timothy Pilgrim
Litigation:	Timothy Pilgrim
Media relations/communications:	Benseon Apple
Policy:	Andrew Hayne
Privacy technology:	Andrew Hayne
Training and education:	Andrew Solomon

Person designated to update this schedule:

Andrew Solomon

Note: All email addresses are simply firstname.lastname@privacy.gov.au


Commissioner
Statutory Office Holder
Karen Curtis
Assistant Commissioner
SES Band 1
Mark Hummerston
Deputy Commissioner
SES Band 2
Timothy Pilgrim
Director, Compliance
EL2
Melanie Drayton
Director, Compliance
EL2
Angelene Falk
Acting Director, Policy
EL2
Andrew Hayne
Acting Director, CaPA
EL2
Andrew Solomon
Enquiries Team Manager
APS6
Karen Garrard
Preliminary Enquiries Team
Acting Dep Director
EL1
Rebecca Jeyasingam
Audit & Data Matching Team
Dep Director
EL1
D'Arcy Jackson
Investigation Team
Dep Director
EL1
Nicole Hunt
Investigation Team
Dep Director
EL1
Andrew Garcia
Investigation Team
Dep Director
EL1
Kristy Burford
Private Sector Team
Dep Director
EL1
Linda King
Health and Access Card Team
Acting Dep Director
EL1
Natasha Roberts
Public Sector Team 1
Dep Director
EL1
Nina Rassaby
Public Sector Team 2 (Cbr)
Dep Director
EL1
Robyn Longhurst
Comms Team
Dep Director
EL1
Benseon Apple
Comms/Web Team
Dep Director
EL1
Martin O'Reilly

Schedule 2

Office of the New Zealand Privacy Commissioner:
Contacts and organisational plan (as at September 2008)

Part A: Contact details

Physical and postal addresses:

Wellington	**Auckland**
Office of the Privacy Commissioner PO Box 10-094 Wellington 6143 New Zealand	Office of the Privacy Commissioner PO Box 466 Auckland 1140 New Zealand
Level 4 109-111 Featherston St	Level 13,WHK Chapman Gosling Tower, 51-53 Shortland St
Tel +64 4 474 7590 Fax +64 4 474 7595	Tel +64 9 302 8680 Fax +64 9 302 2305

Principal liaison person for substantive matters: Blair Stewart +64 9-302 8654

Principal liaison person for administrative matters: Linda Williams + 64 9-302 8680

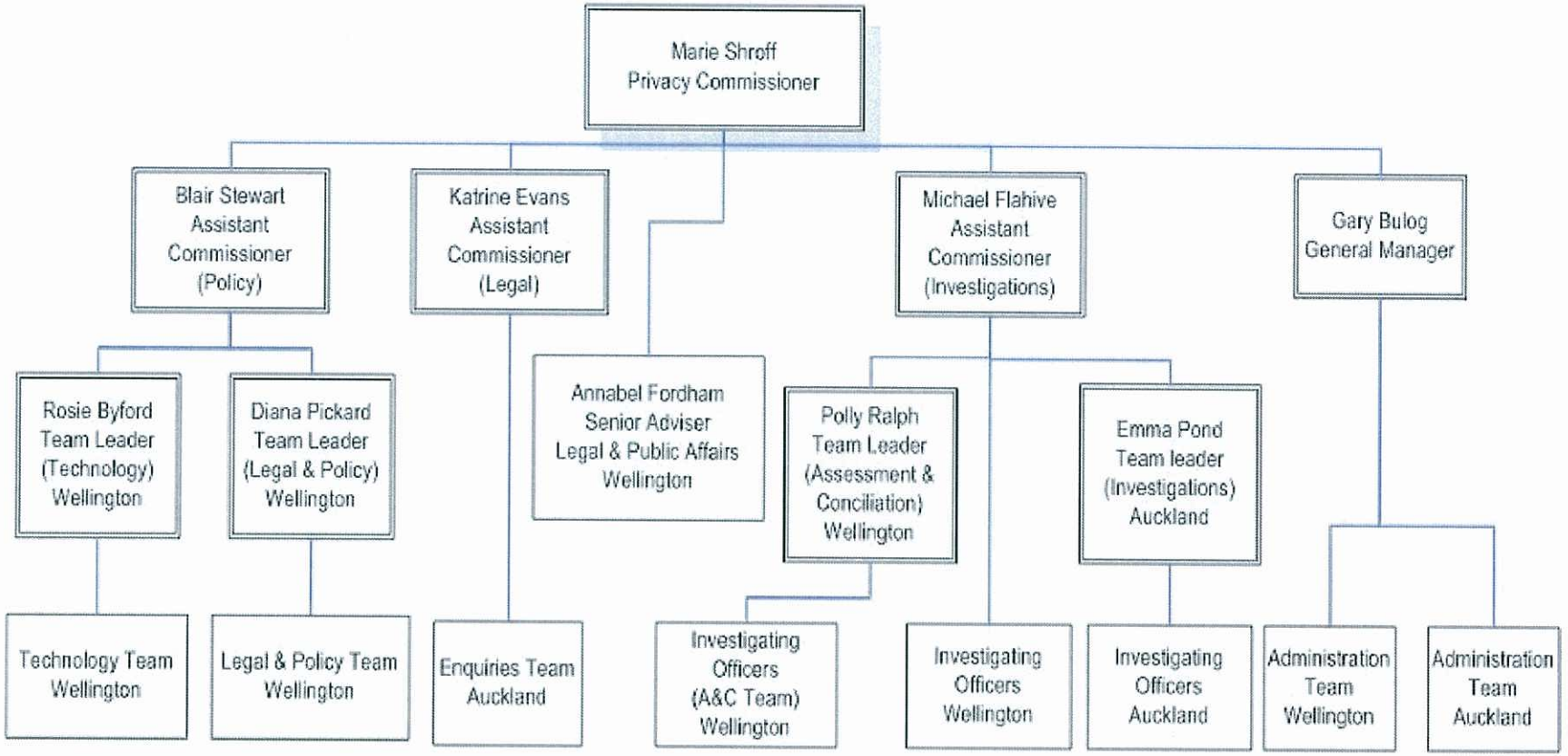
Specialist liaison persons and direct dial contacts:

Codes of practice:	Blair Stewart +64 9-302 8654 (in his absence: Diana Pickard +64 4 -494 7142)
Complaints:	Mike Flahive +64 4-494 7089
Corporate services:	Gary Bulog +64 9-302 8681
Data matching:	Blair Stewart +64 9-302 8654 (in his absence: Rosie Byford +64 4 494 7082)
Legislative issues:	Blair Stewart +64 9-302 8654 (in his absence: Diana Pickard +64 4 -494 7142)
Library:	Gary Bulog +64 9-302 8681 or Blair Stewart +64 9-302 8654
Litigation:	Katrine Evans +64 4-494 7081
Media relations/communications:	Katrine Evans +64 4-494 7081
Policy:	Blair Stewart +64 9-302 8654 (in his absence: Diana Pickard +64 4 -494 7142)
Privacy technology:	Blair Stewart +64 9-302 8654 (in his absence: Rosie Byford +64 4 494 7082)
Training and education:	Katrine Evans +64 4-494 7081

Person designated to update this schedule: Linda Williams +64 9-302 8658

Note: All email addresses are simply firstname.lastname@privacy.org.nz

Office of the Privacy Commissioner



Appendix 1

APEC PRIVACY FRAMEWORK
INTERNATIONAL IMPLEMENTATION
(PART B, I and II)
GUIDANCE FOR INTERNATIONAL IMPLEMENTATION

In addressing the international implementation of the APEC Privacy Framework, and consistent with the provisions of Part A, Member Economies should consider the following points relating to the protection of the privacy of personal information:

I. Information sharing among Member Economies

40. Member Economies are encouraged to share and exchange information, surveys and research in respect of matters that have a significant impact on privacy protection.

41. In furthering the objectives of paragraphs 35 and 36, Member Economies are encouraged to educate one another in issues related to privacy protection and to share and exchange information on promotional, educational and training programs for the purpose of raising public awareness and enhancing understanding of the importance of privacy protection and compliance with relevant laws and regulations.

42. Member Economies are encouraged to share experiences on various techniques in investigating violations of privacy protections and regulatory strategies in resolving disputes involving such violations including, for instance, complaints handling and alternative dispute resolution mechanisms.

43. Member Economies should designate and make known to the other Member Economies the public authorities within their own jurisdictions that will be responsible for facilitating cross-border cooperation and information sharing between economies in connection with privacy protection.

II. Cross-border cooperation in investigation and enforcement

44. Developing cooperative arrangements: Taking into consideration existing international arrangements and existing or developing self-regulatory approaches (including those referenced in Part B. III, below), and to the extent permitted by domestic law and policy, Member Economies should consider developing cooperative arrangements and procedures to facilitate cross-border cooperation in the enforcement of privacy laws. Such cooperative arrangements may take the form of bilateral or multilateral arrangements. This paragraph is to be construed with regard to the right of Member Economies to decline or limit cooperation on particular investigations or matters on the ground that compliance with a request for cooperation would be inconsistent with domestic laws, policies or priorities, or on the ground of resource constraints, or based on the absence of a mutual interest in the investigations in question.

45. In civil enforcement of privacy laws, cooperative cross-border arrangements may include the following aspects:

(a) mechanisms for promptly, systematically and efficiently notifying designated public authorities in other Member Economies of investigations or privacy-enforcement cases that target unlawful conduct or the resulting harm to individuals in those economies;

(b) mechanisms for effectively sharing information necessary for successful cooperation in cross-border privacy investigation and enforcement cases;

(c) mechanisms for investigative assistance in privacy enforcement cases;

(d) mechanisms to prioritize cases for cooperation with public authorities in other economies based on the severity of the unlawful infringements of personal information privacy, the actual or potential harm involved, as well as other relevant considerations;

(e) steps to maintain the appropriate level of confidentiality in respect of information exchanged under the cooperative arrangements.

Appendix 2

Montreux Declaration

« The protection of personal data and privacy in a globalised world: a universal right respecting diversities »

The Data Protection and Privacy Commissioners assembled in Montreux for their 27th International Conference (14 – 16 September 2005) have agreed to promote the recognition of the universal character of data protection principles and have adopted the following final declaration:

1. Following the declaration adopted during the 22nd International Conference of Data Protection and Privacy Commissioners in Venice,

2. Recalling the Resolution on Data Protection and International Organisation adopted during the 25th International Conference of Data Protection and Privacy Commissioners in Sydney,

3. Recognising that the development of the information society is dominated by the globalisation of information exchange, the use of progressively intrusive technologies of data processing and the increase of security measures,

4. Concerned about the growing risks of ubiquitous surveillance of the individual throughout the world,

5. Noting the potential benefits and risks inherent in new technologies of information,

6. Concerned by the current disparities between the legal systems in different parts of the world and in particular the absence of data protection safeguards in some places that undermines effective global data protection,

7. Aware that the fast increase in knowledge in the field of genetics may make human DNA the most sensitive personal data of all; aware also that this acceleration in knowledge raises the importance of adequate legal protection of these data,

8. Recalling that the collection and any subsequent processing of personal data must be done with regard to the requirements of data protection and privacy,

9. Recognising the need in a democratic society to efficiently fight terrorism and organised crime, but reminding that this purpose can be achieved in the best possible way when human rights and in particular human dignity are respected,

10. Convinced that the right to data protection and privacy is an essential condition in a democratic society in order to safeguard the respect for the rights of the people, a free flow of information and an open market economy,

11. Convinced that the right to data protection and privacy is a fundamental human right,

12. Convinced that it is necessary to strengthen the universal character of this right in order to obtain a universal recognition of the principles governing the processing of personal data whilst respecting legal, political, economical and cultural diversities,

13. Convinced of the need to guarantee individual rights to all citizens of the world without discriminations wherever and whenever their personal data are processed,

14. Recalling that the World Summit on the Information Society 2003 in Geneva in its Declaration of Principles and Plan of Action has underlined the importance of data protection and privacy for the development of the information society,

15. Recalling the recommendation of the International Working Group on Data Protection in Telecommunications to take into account the Decalogue, worked out in 2000, in order to protect privacy in the frame of multilateral privacy agreements,

16. Recognising that the principles of data protection derive from international legal binding and non-binding instruments such as the OECD Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, the United Nations Guidelines concerning Computerized Personal Data Files, the European Union Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and the Asia Pacific Economic Cooperation Privacy Framework,

17. Recalling that these principles are in particular the following:

- Principle of lawful and fair data collection and processing,
- Principle of accuracy,
- Principle of purpose-specification and -limitation,
- Principle of proportionality,
- Principle of transparency,
- Principle of individual participation and in particular the guarantee of the right of access of the person concerned,
- Principle of non-discrimination,
- Principle of data security,
- Principle of responsibility,
- Principle of independent supervision and legal sanction,
- Principle of adequate level of protection in case of transborder flows of personal data.

Accordingly,

The Data Protection and Privacy Commissioners express their will to strengthen the international recognition of the universal character of these principles. They agree to collaborate in particular with the governments and international and supra-national organisations for the development of a universal convention for the protection of individuals with regard to the processing of personal data.

To this end, the Commissioners appeal:

a. to the United Nations to prepare a legal binding instrument which clearly sets out in detail the rights to data protection and privacy as enforceable human rights;

b. to every Government in the world to promote the adoption of legal instruments of data protection and privacy according to the basic principles of data protection;
c. to the Council of Europe to invite, in accordance with article 23 of the Convention for the protection of individuals with regard to automatic processing of personal data, non-member-states of the Council of Europe which already have a data protection legislation to accede to this Convention and its additional Protocol.

The Commissioners also appeal:

a. to international and supra-national organisations to commit themselves to complying with principles that are compatible with the principal international instruments dealing with data protection and privacy and in particular to establish operationally independent supervisory authorities with control powers;
b. to those international Non-Governmental Organisations, such as business and consumers associations to develop standards based on or consistent with the fundamental principles of data protection;
c. to hardware and software manufacturers to develop products and systems integrating privacy enhancing technologies.

Furthermore, the Commissioners agree:

a. to intensify in particular the exchange of information, the coordination of their supervisory activities, the development of common standards, the promotion of information concerning the activities and resolutions of this conference;
b. to promote cooperation with countries which do not yet have independent supervisory data protection authorities;
c. to promote the exchange of information with international Non Governmental Organisations which are dealing with data protection and privacy;
d. to collaborate with the data protection officers of organisations;
e. to create a permanent website in particular as a common base for information and resources management.

The Data Protection and Privacy Commissioners agree to assess the realisation of the objectives of this declaration on a regular basis, with the first evaluation taking place at the 28th International Conference in 2006.

Appendix 3
Asia Pacific Privacy Authorities Forum
Statement of Objectives

Meeting in Melbourne, Australia, on 17 November 2005, the assembled privacy authorities from Australia, Hong Kong, Korea and New Zealand, resolved as follows:

RECOGNISING that:

- Privacy is a matter of growing international concern
- Information networks closely connect people and organisations in our various jurisdictions regardless of physical borders and differing laws
- Governments and business expect regulators to strive for efficient and effective solutions and that best practice requires privacy authorities to be aware of what similar regulators are doing
- Privacy issues can emerge in one jurisdiction before others and that privacy authorities can benefit from an advanced warning system
- Privacy authorities are increasingly being called upon to contribute to solutions to complaints, or policy challenges, that cross borders
- There is limited specialised data privacy resource in any one jurisdiction and that privacy authorities benefit from reaching abroad for information, inspiration and assistance
- Participants in the forum will benefit from cooperation in information privacy knowledge sharing and technical resources
- Adoption of the APEC Privacy Framework in 2004 has provided a regional restatement of the importance of privacy and transborder information flows and a spur to reinvigorate regional cooperative arrangements

THEREFORE we resolve to:

- Continue the cooperative arrangements established in 1992 and which came to be known as PANZA+ in the ensuing 24 meetings
- Rename the meeting as the Asia Pacific Privacy Authorities Forum
- Encourage further participation from within the region

AND FURTHER RESOLVE to build upon and enhance the current arrangements with the principal objectives of:

- Facilitating the sharing of knowledge and resources between privacy authorities within the region
- Fostering cooperation in privacy and data protection
- Promoting best practice amongst privacy authorities
- Working to continuously improve our performance to achieve the important objectives set out in our respective privacy laws.

Privacy Commissioner of Australia
Privacy Commissioner of New Zealand
Privacy Commissioner for Personal Data, Hong Kong SAR
Privacy Commissioner of New South Wales, Australia
Privacy Commissioner of Victoria, Australia
Information Commissioner of Northern Territory, Australia
Korea Information Security Agency

Appendix 4
OECD Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy

Clause 13 International co-operation

Member countries and their Privacy Enforcement Authorities should co-operate with each other, consistent with the provisions of this Recommendation and national law, to address cross-border aspects arising out of the enforcement of Laws Protecting Privacy. Such co-operation may be facilitated by appropriate bilateral or multilateral enforcement arrangements.