privacynsw

Privacy NSW
Office of the NSW
Privacy Commissioner

Locked Bag 5111
Parramatta NSW 2124

Justice Precinct Offices
160 Marsden Street
Parramatta NSW 2150

Phone (02) 8688 8585
Fax (02) 8688 9660

www.lawlink.nsw.gov.au/privacynsw

ISSN 1448-4609

PRIVACY NSW Annual Report 2006 2007

privacynsw

PRIVACY NSW
Annual Report 2006 2007

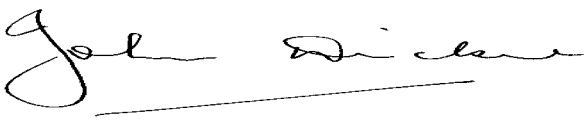
privacynsw
Office of the NSW Privacy Commissioner

The Hon. John Hatzistergos
Attorney General and Minister for Justice
Parliament House
Sydney NSW 2000

Dear Attorney,

In compliance with section 64 of the *Privacy and Personal Information Protection Act 1998*, I submit the Annual Report of Privacy NSW for the reporting year 2006-2007.

Yours faithfully



John Dickie
(Acting) Privacy Commissioner

Contents

From the Commissioner

During the last year privacy law in Australia and New Zealand has been coming under increasing scrutiny.

There are at present four Law Reform Commissions – three in Australia - and the fourth in New Zealand looking at how the law can be improved.

The common task linking the inquiries is to adapt privacy law to take account of the huge leaps in technological change since the laws were originally introduced; then, if possible, to simplify the laws and finally to bring a sense of harmony into those laws across the jurisdictions.

It is therefore a time of great opportunity for all of us to help form a framework to make it easier for people in the community to understand what the law of privacy is about, easier for them to invoke it if they feel their privacy has been invaded and easier to administer the laws more effectively.

There have already been some significant developments. The Australian Law Reform Commission has put out for comment a 600 page Issues Paper dealing in great detail with the federal privacy legislation. The New South Wales Commission has published a Consultation Paper on whether there should be a statutory cause of action for privacy in New South Wales.

Both of these Commissions are working closely so that wherever possible there will be no duplication of effort, which means, for instance, that although the statutory cause of action question is primarily relevant to the New South Wales LRC, it will also figure in the ALRC's final report and as such will come into national calculations.

It is significant that in both references made to the Commissions both the Commonwealth Attorney General and the New South Wales Attorney General emphasised the co-operative aspects of the inquiries.

The Commonwealth reference asks the ALRC to consult with relevant stakeholders, including the Office of the Privacy Commissioner, relevant State and Territory bodies and the Australian business community and to ensure widespread public consultation.

The NSW reference speaks of the desirability of privacy protection principles being uniform across Australia and asks the Commission to liaise with the ALRC as well as other relevant Commonwealth, State and Territory agencies.

A further step was taken in the direction of uniformity when the two references were brought officially to the Standing Committee of Attorneys General with the purpose of coordination in mind. The New Zealand Attorney General is a member of that Committee.

Because of the different roles of the privacy agencies in Australia and in New Zealand, the ideal solution to the harmonisation of privacy laws would not be for uniform legislation but interlocking legislation which would spell out the different functions based on the one set of privacy principles.

Other matters which the Commissions will be looking at include the physical aspects of privacy and how these can be included in the new look legislation.

An indication of how the members of the community think of privacy legislation was the result of a phone in by the ALRC which indicated by far the most outstanding issue was telephone marketing outside of normal hours.

Indications from telephone complaints also suggest that other acts of physical privacy, particularly those related to closed circuit television cameras and photographs from mobile phones are of an increasing concern.

Other privacy intrusive conduct regulated already by legislation, such as the laws governing listening devices and surveillance in the workplace would also have a more appropriate home in privacy legislation. This would mean that those in the community who have legitimate concerns about these matters could raise them as complaints under a revised privacy act.

There is good reason for optimism that if the legislators get it right, it will greatly improve the administration of privacy not only in Australia but in the East Asia and Pacific area as well.

Twice a year Privacy Commissioners from Australia, New Zealand and Hong Kong and officials from Korea meet to thrash out emerging problems and how best to deal with them.

This occurs during the APPA Forum – the meeting of the Asia Pacific Privacy Authorities.

There is a genuine spirit of cooperation among the privacy commissioners to keep ahead of the game in dealing with privacy related issues and to see that legislators are made aware of the significant developments in technology which are privacy intrusive.

At the second meeting in Cairns this year, it was foreshadowed that other countries might be about to sign up to become members of the Forum.

The first joint project was to plan for an international Privacy Awareness Week to be celebrated in each of the countries making up APPA. Victoria has been observing Privacy Awareness Week for six years but now the idea has been adopted with enthusiasm by the rest of Australia and by the other APPA members.

The project to mark the week this year has been an international competition for secondary students setting out in either essay, blog or poetic form what privacy means to them. The winner will be announced in Privacy Awareness Week after the Privacy Commissioners have judged the winning entries.

The competition itself and the willingness and capacity of the different members of APPA to make it successful indicate that on a wider canvas, a great deal can be achieved.

It is why a rethinking of our privacy laws and harmonising them to the greatest extent possible can make the benefits from them accessible and workable for the communities within our region.

Theme for Annual Report

In the early stirrings about privacy late in the nineteenth century, the two American scholars, Warren and Brandeis adopted and brought into the vernacular Judge Cooley's observation that privacy is "the right to be let alone."

Since then, and especially in the last three or four decades when technology has made such enormous progress, we have tended to regard our personal information and data protection as the most important aspects of our privacy.

Certainly this has been the emphasis of national and international laws on the subject.

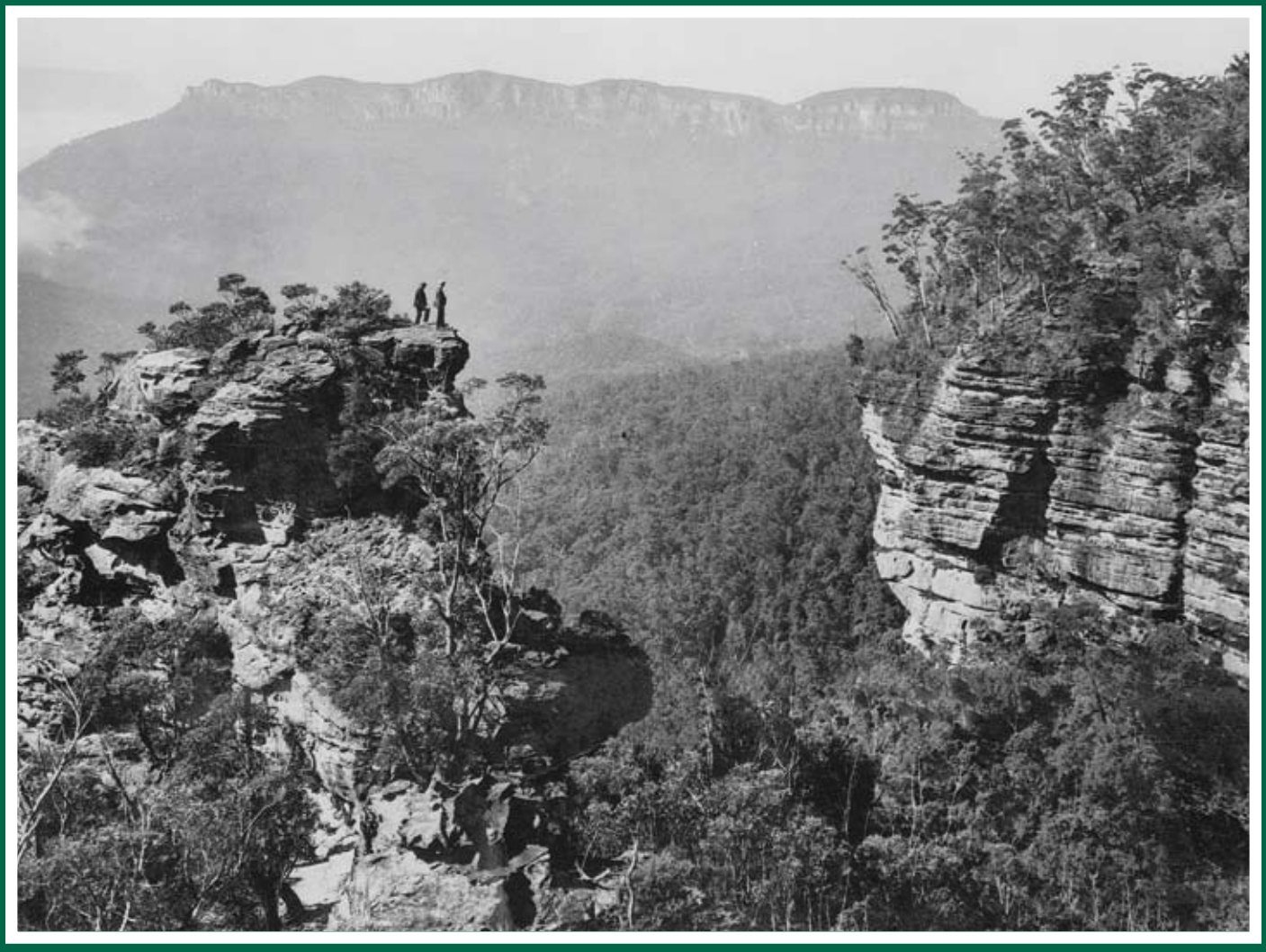
Yet to many people, the right to enjoy solitude, to proceed at one's own pace and have the time to contemplate remains as important as it ever was.

We have devoted some space to this concept in this Report and we have tried to do it with pictures rather than with words.

For those of you who fancy sitting on a chair on a headland looking at the ocean, or contemplate a garden in early spring or who sit in a boat at the end of a line waiting for a bite, we hope it resonates.

The cover picture is of a tree at Cobar in the north west of New South Wales. We have chosen it to represent the solitude and time for contemplation I consider so important.

John Dickie
ACTING PRIVACY COMMISSIONER



Copelands Lookout and Mount Solitary, Jamieson Valley (NSW)

The role of Privacy NSW is to:

- educate the people of NSW about the meaning and value of privacy and to assist them in the protection and enhancement of that privacy;
- promote the adoption of best privacy practice by all holders of personal data, particularly NSW Government agencies, thereby promoting an increased level of trust.

Privacy NSW protects privacy in the following ways:

- by advising individuals, government agencies, business and other organisations on what steps they should take to ensure that the right to privacy is protected;
- by researching significant developments in policy, law and technology which may have an impact on privacy and by making reports and recommendations to relevant authorities;
- by answering enquiries and educating the community about privacy issues;
- by advising people of possible remedies for breaches of their privacy;
- by receiving, investigating and conciliating complaints about breaches of privacy;
- by overseeing the conduct of Internal Reviews by NSW Government Agencies into privacy complaints;
- by appearing in the Administrative Decisions Tribunal in appeals dealing with internal reviews.

How to Contact Privacy NSW

Mail Locked Bag 5111
Parramatta NSW 2124

Office Justice Precinct Offices
160 Marsden Street
Parramatta NSW 2150

Phone (02) 8688 8585

Fax (02) 8688 9660

Email privacy_nsw@agd.nsw.gov.au

Website www.lawlink.nsw.gov.au/privacynsw

Hours of business are 9.00 am to 4.30 pm Monday to Friday.

Privacy NSW Who it is and what it does

The Office of the NSW Privacy Commissioner (Privacy NSW) was established in February 1999 under the *Privacy and Personal Information Protection Act 1998* (PPIPA).

The highlights of this year's work by the office are diverse. The core work of PNSW includes advising individuals, government agencies, businesses and other organisations on steps they should take to ensure basic rights of privacy are protected and overseeing the complaint-handling procedures enshrined in privacy legislation. The office has however also committed a major portion of its time to making submissions to the Australian Law Reform Commission and the NSW Law Reform Commission. Harmonisation of privacy laws has become a central concern for the office, as both Commissions have recognised that the community finds it difficult to understand privacy law and its complexity.

Protection of Privacy

Members of the community expect that privacy law will apply not only to their personal information but also to their physical privacy. They are concerned at the way CCTV cameras can be turned upon their homes, how cameras, either on their own or on mobile telephones, can take intrusive digital photographs, how their evenings can be interrupted by telemarketing calls and by the spam mail which often clogs their email systems.

Harmonisation of privacy laws

Central to this year's work are the privacy references to the Australian Law Reform Commission and the New South Wales Law Reform Commission. These provide a unique opportunity to build a comprehensive and unified privacy regime throughout Australia.

The references represent the chance to make the law more comprehensible to the people it is designed to protect, to eradicate the areas of overlap between the Commonwealth and the States and to include under the privacy umbrella intrusive and unwelcome invasions of people's personal space (one of the problems is the multiplicity of privacy principles varying in number between Commonwealth, State and Territory legislation – most of them traversing similar issues).

At the moment, there is also a reference on privacy issues to the New Zealand Law Reform Commission. One of the major matters in that reference is the harmonisation of privacy laws with Australia. It would be remiss if an opportunity was missed to have the same laws on either side of the Tasman.

As part of the work of the Law Reform Commissioners the following meetings were held in which Privacy NSW took part:

Public Meeting on Privacy and You

On 26 March 2007, as part of Law Week 2007 celebrations, the New South Wales Law Reform Commission held a public seminar on a person's right to privacy. All interested members of the public and legal profession were invited to attend.

Public Meeting on Privacy in Business

During the reporting year, the Australian Law Reform Commission and the New South Wales Law Reform Commission held a public meeting on this topic as part of their review of privacy law in Australia and staff of Privacy NSW attended.

Submission to ALRC

Privacy NSW made a submission to the Australian Law Reform Commission in response to the Issues Paper circulated by the ALRC entitled "ALRC Issues Paper 31, October 2006 *Review of Privacy* (IP31).

Education & Research

Privacy NSW aims to educate the people of New South Wales about the meaning and value of privacy and assist in protecting and enhancing that privacy. This year PNSW released the PPIP Act Training Program online for Privacy Contact Officers in government agencies.

During the 2006 - 07 financial year, the members of the Asia Pacific Privacy Authorities (APPA) were Australia, New Zealand, Hong Kong, Korea, British Columbia, Northern Territory, Victoria and New South Wales (Canada joined APPA subsequently). This year APPA sponsored an international competition for secondary school students on issues surrounding privacy. Secondary school students were chosen because this age group is often seen as lacking in privacy awareness e.g. their willingness to give-away private information on websites such as MySpace™ and YouTube™. Students were competing for prizes which included a laptop computer and gift vouchers.

Consultation & Partnerships

Privacy and Information Commissioners in Australia have a strong bond with other Privacy, Data Protection and Information Commissioners through APPA. This year a senior officer of PNSW attended the meeting of the 28th International Conference of Data Protection and Privacy Commissioners in London and the meeting of the Asia Pacific Privacy Authorities (APPA) Conference in Hong Kong.

Throughout the year, PNSW also hosted meetings of the NSW Privacy Advisory Committee. This Committee advises the Privacy Commissioner on matters relevant to his / her functions, recommends material to the Privacy Commissioner for inclusion in guidelines and advises the Minister on such matters as may be referred to the Committee by the Minister.

Legislative initiatives undertaken in partnership with other agencies

Privacy NSW assisted in the revision of the Guidelines on Disclosure of Information During Industrial Consultations issued by the Premier's Department. The previous Guidelines were based on the requirements for disclosure of personal information established by the *Privacy and Personal Information Protection Act 1998* (the PIPPA) and were originally distributed in Circular C2003-50. The Guidelines (C2007-27) have now been updated to include consideration of the *Health Records and Information Privacy Act 2002* (the HRIP Act). The Guidelines recognise that industrial relations and occupational health and safety legislation may require personal and/or health information to be disclosed in certain circumstances. The Guidelines are available on the website of Privacy NSW whose address is: www.lawlink.nsw.gov.au/privacynsw.

Directions/Exemptions under section 41 of PPIPA or section 62 of HRIPA

Developing and renewing section 41 Directions under the PPIP Act 1998 was also a major component of our work during this reporting year. Under section 41 of the PPIP Act, the Privacy Commissioner may make a Direction to waive or modify the application of one or more of the IPPs by one or more NSW public sector agencies. Agencies may approach the Privacy Commissioner to request a public interest Direction, or the Privacy Commissioner may recognise a need for a public interest Direction without a request.

Public interest Directions are temporary in nature. This allows the affected agency or agencies some time, in which to either amend their practices and procedures to bring them into compliance with the IPPs; to draft a privacy code of practice or to enact legislation exempting them from the IPPs. If the Privacy Commissioner is satisfi ed that the public interest in making an exemption outweighs the public interest in having agencies comply with the privacy principles, the Privacy Commissioner will cause a Direction to be drafted. The draft Direction may then be the subject of a further round of consultation.

Finally the Privacy Commissioner must submit the draft Direction to the relevant minister, and seek the relevant Minister's approval of the direction. Once the Privacy Commissioner has made a direction, it is placed on the Privacy NSW website. The relevant Minister for the PPIP Act is the NSW Attorney General. The Attorney General must also be consulted about exemptions to be made under the HRIP Act and the Minister whose approval must be sought in that case is the Minister of Health.

The section 41 Directions made between 30 June 2006 and 30 June 2007 include:

- **Direction relating to the Anti-Social Behaviour Pilot Project.** This Direction operates from 30 April 2007 until the completion of the Project, and replaces the previous Direction relating to the Case Coordination Partnership Project. A related Direction has been made under section 62 of the HRIP Act.
- **Direction on the Incidental Disclosure and the Transfer of Personal Information belonging to Third Parties to the (SA) Commission of Inquiry into Children in State Care.** This Direction applies to the Department of Community Services in relation to the South Australian Commission of Inquiry into Children in State Care. It operates from 15th November 2006 to 31st December 2006 or until the expiry of the South Australian Commissioner's Terms of Reference, whichever is the later. A related Direction has been made under section 62 of the HRIP Act.
- **Direction relating to the Child Protection Watch Team Trial.** This Direction applies to agencies participating in the Child Protection Watch Team Trial. It was made on 7 August 2006 and has effect for until the completion of the CPWT Trial.

The seven sector wide Directions under PPIPA which were renewed in December 2006 are:

- **Indirect Collection of Information about Third Parties by Human Service Agencies.** This direction replaced the Direction on the Better Service Delivery Program. It was initially made to commence on 1 July 2003 and affects some health, education, welfare, housing, juvenile justice and Aboriginal affairs agencies. On 29 December 2006 it was extended to 31 December 2007.
- **Disclosures to the National Coronial Information System.** This Direction affects some health and justice agencies. It was originally made on 18 February 2002 and on 29 December 2006 was extended to 31 December 2007.
- **Collection and disclosure for research purposes.** This Direction affects most NSW state agencies. It was originally made on 30 June 2000 and on 29 December 2006 was extended to 31 December 2007.
- **Disclosure of Information to Victims of Crime.** This Direction affects many law enforcement and justice agencies. It was originally made on 28 September 2000. On 29 December 2006 it was extended to 31 December 2007.

- **The Department of Ageing, Disability and HomeCare, the Guardianship Tribunal and the Disability Council.** Originally made on 30 June 2000, this Direction was extended on 29 December 2006 to 31 December 2007. The original Direction was substantially modified in later versions.

- **The use of information for investigative purposes.** This Direction covers most NSW state agencies. It was originally made on 30 June 2000. On 29 December 2006 it was extended to 31 December 2007.

- **Some information transfers between public sector agencies.** This Direction covers most NSW state agencies. It was originally made on 30 June 2000. On 29 December 2006 it was extended to 31 December 2007.

Two Exemptions / Directions were made under HRIPA during the reporting period:

- **Direction relating to the Anti-Social Behaviour Pilot Project**
  The Direction operates from 30 April 2007 until the completion of the Project, and replaces the previous Direction relating to the Case Coordination Partnership Project. A related Direction has been made under section 41 of the PPIP Act.

- **Direction on the Incidental Disclosure and the Transfer of Health Information belonging to Third Parties to the (SA) Commission of Inquiry into Children in State Care**
  This Direction applies to the Department of Community Services in relation to the South Australian Commission of Inquiry into Children in State Care. It operates from 15th November 2006 to 31st December 2006 or the expiry of the South Australian Commissioner's Terms of Reference, whichever is the later. A related Direction has been made under section 41 of the PPIP Act.

Codes of Practice

During the reporting period, amendments were made to the Privacy Code of Practice (General) 2003 and the various Codes of Practice developed in previous years remain in force. These codes are approved by the relevant minister(s) and allow an agency to modify or waive the application of the privacy principles and/or the public register provisions. The Codes currently in force under the PPIP Act are:

- Privacy Code of Practice (General) 2003 - amendments include Part 4 dealing with Human Services made and commenced 1 July 2005. Part 5 dealing with Corrective Services and Part 6 dealing with Ageing, Disability and Home Care Services were commenced on 15 September 2006.

- Privacy Code of Practice for the Bureau of Crime Statistics and Research

- Privacy Code of Practice for the Workforce Profile

- Privacy Code of Practice for Local Government

- Privacy Code of Practice for the Office of the Director of Public Prosecutions

- Department of Education and Training: Privacy Code of Practice

- NSW Police Service Privacy Code of Practice

- Department of Housing Privacy Code of Practice

- Privacy Code of Practice for the Legal Aid Commission

- Privacy Code of Practice for the Department of Fair Trading

The Code in force under the HRIP Act is:

- The Health Records and Information Privacy Code of Practice 2005.

What is privacy?

There is no simple definition of privacy to cover all circumstances. A number of elements may be considered, such as the right to a sense of personal autonomy; the right to have information about oneself used fairly and, traditionally, a 'right to be left alone'. Many people confuse privacy with secrecy or confidentiality but privacy is broader than both of these.

Increasingly, privacy protection is focusing on the need to ensure the fair use of personal information. The fair use of personal information is an essential element of an information economy, just as the fair use of money is an essential element of the financial economy.

In other instances one could refer to the influential definition of privacy developed by the American legal academic William Prosser (the Prosser test). This test treats the following as breaches of privacy:

- the intrusion upon a person's seclusion or solitude, or into their private affairs
- public disclosure of embarrassing facts about a person
- publicity which places a person in a false light in the public eye
- appropriation of a person's name or likeness.

"South Solitary Lighthouse" NSW
South Solitary Island lying 18km north-east off Coffs Harbour was regarded as the most isolated place in NSW.
Photograph courtesy of Mr Ian Clifford

About the Privacy and Personal Information Protection Act 1998 (NSW)

The *Privacy and Personal Information Protection Act 1998* (the PPIP Act) deals with the way public sector agencies in NSW manage personal information. It was passed in 1998 to provide the people of NSW with enforceable privacy rights.

The PPIP Act applies to 'personal information', which is defined broadly to mean information or an opinion about an individual, whose identity is apparent or can be ascertained from the information or opinion. 'Public sector agencies' are broadly defined by the PPIP Act to include government departments, statutory or declared authorities, the police service, local councils, and bodies whose accounts are subject to audit by the Auditor General.

The PPIP Act sets out 12 Information Protection Principles (IPPs), which are the backbone of the Act. The primary mechanism for enforcement of the IPPs is for individuals to seek an 'internal review' of an agency's conduct or decision, which may have been in breach of one or more of the IPPs.

The PPIP Act also established the Office of the Privacy Commissioner and assigns to the Commissioner functions that in the past were carried out by the NSW Privacy Committee. These functions include conducting research, providing advice and handling complaints about breaches of privacy. The Privacy Commissioner was also given new functions (e.g. overseeing internal reviews and assisting the Administrative Decisions Tribunal in privacy cases) and additional powers (e.g. Royal Commission powers of investigation).

What is personal information?

The PPIP Act defines personal information as any information or opinion that relates to an identifiable person. This definition covers not only traditional areas of data storage, such as paper files but also includes such things as an individual's fingerprints, retina prints, body samples or genetic characteristics.

The Act excludes certain types of information from the definition of personal information, such as:

- information contained in a publicly available publication
- information about an individual's suitability for public sector employment
- information about people who have been dead for more than 30 years.

The Information Protection Principles

One of the main purposes of the Act was to introduce the Information Protection Principles (IPPs); a set of privacy standards that regulate the way NSW public sector agencies must deal with personal information.

The IPPs reflect international standards for the protection of personal information. They are based on the National Privacy Principles (NPPs) in the Commonwealth *Privacy Act 1988* which in turn are based on the Organisation for Economic Cooperation and Development's (OECD) 1981 Guidelines on the Protection of Privacy and the Transborder Flows of Personal Data.

The IPPs regulate the collection, storage, access, use and disclosure of personal information by NSW public sector agencies.

The IPPs can be summarised as:

Collection

1. **Lawful –** only collect personal information for a lawful purpose. Only collect the information if it is directly related to the agency's activities and necessary for that purpose.
2. **Direct –** only collect information directly from the person concerned, unless they have given consent to do otherwise. Parents and guardians can give consent for minors.
3. **Open –** inform the person as to what information is being collected, why it is being collected and who will be storing and using it. Agencies must also inform the person how they can see and correct this information.
4. **Relevant –** ensure that the information is relevant, accurate, not excessive and up-to-date. Ensure that the collection does not unreasonably intrude into the personal affairs of the individual.

Storage

5. **Secure –** ensure that personal information is stored securely, not kept any longer than necessary and disposed of appropriately. Information should be protected from unauthorised access, use or disclosure.

Access

6. **Transparent –** explain to the individual what personal information about them is being stored, why it is being used and any rights they have to access it.
7. **Accessible –** allow people to access their personal information without unreasonable delay and without expense.
8. **Correct –** allow people to update, correct or amend their personal information where necessary.

Use

9. **Accurate –** ensure that the personal information is relevant and accurate before using it.
10. **Limited –** only use personal information for the purpose for which it was collected, for a directly related purpose, or for a purpose to which the individual has given consent. Personal information can be used without consent in order to deal with a serious and imminent threat to any person's health or safety.

Disclosure

11. **Restricted –** only disclose personal information if the person has given their consent or if they were informed at the time of collection that it would be disclosed in this way. Information can only be disclosed for a related purpose if it is believed that the person concerned is not likely to object. Personal information can be disclosed without consent in order to deal with a serious and imminent threat to any person's health or safety.
12. **Safeguarded –** do not disclose sensitive personal information without consent, for example, information about a person's ethnic or racial origin, political opinions, religious or philosophical beliefs, sexual activities or trade union membership. Sensitive information can only be disclosed without consent in order to deal with a serious and imminent threat to any person's health or safety.

It should be noted specifi c legislation can modify or override any of the above IPPs. In addition an exemption or Privacy Code of Practice may be relevant to their interpretation.

About the Health Records and Information Privacy Act 2002 (NSW)

The *Health Records and Information Privacy Act 2002* (the HRIP Act) creates a scheme for the collection and handling of health information by both public and private sector organisations in New South Wales. It applies to most NSW organisations and to health providers who collect, hold or use health information.

Together with the *Privacy and Personal Information Protection Act 1998* (PPIP Act), the HRIP Act offers the people of NSW a complete regime of enforceable privacy rights.

The intent of the HRIP Act is to:

- protect the privacy of an individual's health information held in both the public and private sectors
- balance the public interest in protecting the privacy of health information with the public interest in the legitimate use of that information
- enhance the ability of individuals to be informed about their health care
- establish an accessible framework to resolve complaints about the handling of health information.

The definition of a 'public sector agency' is similar to that found in the PPIP Act. An 'organisation' is defined in the Act to include a public sector agency or a private sector person or company. This means that individuals (such as GPs) are covered by the HRIP Act. It also means that the HRIP Act applies to both the NSW public and private sector.

More specifically, under the HRIP Act, a health service provider is defined to mean any organisation that provides a health service, except an organisation that merely arranges for a health service to be provided to a person by another organisation.

Health services may include:

- medical, hospital and nursing
- dental
- mental health
- pharmaceutical
- ambulance
- community health
- health education
- podiatrist services
- services provided by naturopaths, therapists and alternative health care.

The HRIP Act sets out 15 Health Privacy Principles (HPPs), which are central to the Act.

The primary mechanism for enforcement of the HPPs in the public sector is for individuals to seek an 'internal review' of a NSW agency's conduct or decision, which may have been in breach of one or more of the HPPs. The mechanism for enforcement of the HPPs in the private sector is for individuals to initiate a complaint for investigation and conciliation by the NSW Privacy Commissioner.

Under the HRIP Act, the NSW Privacy Commissioner carries out similar functions to those assigned her/him by the PPIP Act. These functions include conducting research, providing advice and handling privacy complaints.

The Health Privacy Principles

The main purpose of the Act was to introduce the Health Privacy Principles (HPPs). The HPPs embody a set of privacy standards that regulate the way in which private sector organisations and public sector agencies in NSW must deal with health information.

The HPPs can be summarised as:

Collection

1. **Lawful –** when an organisation collects health information, the information must be collected for a lawful purpose, directly related to that organisation's activities and necessary for that purpose.

2. **Relevant –** the organisation must ensure that health information is relevant, accurate, up to date and not excessive. The collection should not unreasonably intrude into an individual's personal affairs.

3. **Direct –** health information must be collected directly from the individual concerned, unless it is unreasonable or impracticable for the organisation to do so.

4. **Open –** the individual must be informed why the health information is being collected, what will be done with it, and who else might see it. The individual must also be informed how to access and amend their health information and the consequences, if the organisation fails to provide the health information.

   If an organisation collects health information about a person from someone else, it must still take reasonable steps to ensure that the person, whose health information it is, is aware of the above points.

Storage

5. **Secure –** the organisation must ensure that health information is stored securely, not kept any longer than necessary, and disposed of appropriately. It should be protected from unauthorised access, use or disclosure.

Access & Accuracy

6. **Transparent –** the organisation must provide an individual with details about what health information about them is being stored, why the organisation is storing it and what rights the individual has to access it.

7. **Accessible –** the organisation must allow people to access their health information without unreasonable delay or expense.

8. **Correct –** the organisation must allow people to update, correct or amend their health information where necessary.

9. **Accurate –** the organisation must ensure that a person's health information is relevant and accurate before using or disclosing it.

Use

10. **Limited –** an organisation can only use health information for the purpose for which it was collected or for a directly related purpose, which a person would reasonably expect. Otherwise the health information can only be used with consent (unless one of the exemptions in HPP 10 itself applies).

Disclosure

11. **Limited –** an organisation can only disclose health information for the purpose for which it was collected, or a directly related purpose, which a person would reasonably expect. Otherwise it can only be disclosed with consent (unless one of the exemptions in HPP 11 applies).

Identifi ers & Anonymity

12. **Not identifi ed –**an organisation can only give an individual an identifi cation number if it is reasonably necessary to carry out the organisation's functions effi ciently.

13. **Anonymous –** a person is entitled to receive health services anonymously, where this is lawful and practicable.

Transferrals and Linkage

14. **Controlled –** health information can only be transferred outside New South Wales if the receiving jurisdiction has health privacy laws similar to that of New South Wales. Otherwise it can only be transferred with consent (unless one of the other stipulations in HPP 14 applies).

15. **Authorised –** health information can only be included in a system to link health records across more than one organisation with the express consent of the individual.

Note

Specifi c legislation can also modify or over-ride the above HPPs and exemptions or Privacy Codes of Practice may be relevant to their interpretation.

What is health information?

The HRIP Act defi nes health information as any information or opinion that relates to:

- a person's health, either physical or mental or a disability
- expressed wishes as to the provision of services
- any health services which have been provided, or which may be provided in the future.

The defi nition of health information includes personal information collected in order to provide a health service, such as contact details.

Under the HRIP Act, the defi nition of health information also includes information connected with organ donation, body parts, and genetic information.

The Act excludes certain types of information from the defi nition of health information, such as:

- information contained in a publicly available publication
- information about an individual's suitability for public sector employment
- information about people who have been dead for more than 30 years
- information in an individual's employee record held by a private sector person.

Complaints and Internal Reviews

Under the existing privacy regime in NSW there are two avenues of complaint available to individuals who believe that their privacy has been breached:

- Under Part 4 of the *Privacy and Personal Information Protection Act 1998* (PPIP Act) and parts 6 and 7 of the *Health Records and Information Privacy Act 2002* (HRIP Act), Privacy NSW is responsible for accepting and considering complaints made by individuals who believe their privacy may have been violated or interfered with.
- Under Part 5 of the PPIP Act which is referred to in Part 3 of the HRIP Act, those who believe that a NSW public sector agency has breached either Act can direct their complaints directly to the agency and request that the agency conduct an internal review of the behaviour that may have lead to the complaint. Privacy NSW is responsible for the oversight of internal reviews.

The complaints received by Privacy NSW range from the handling of personal or health information by State Government agencies and private sector organisations to neighbourhood disputes. Generally we will not investigate a complaint unless it has been lodged in writing and we will not investigate a complaint that has already been lodged elsewhere.

Having received a complaint, Privacy NSW may undertake a preliminary assessment of the complaint. We may decline to investigate a complaint if it is considered frivolous, vexatious, trivial, lacking in substance, not made in good faith or if it can be resolved by referral to a more appropriate agency.

Complaint Handling and Referral

Privacy NSW is party to an Information Sharing Arrangement and Complaint Referral Arrangement with the NSW Ombudsman, the Health Care Complaints Commissioner, the Anti-Discrimination Board and the Legal Services Commissioner.

These Arrangements enable the signatory agencies to refer a complaint to another agency if that agency has the power to deal with it. Privacy NSW therefore passes a complaint to another government body if we feel that we are not the best organisation to deal with the complaint and if the complainant gives their express consent to do so.

Information Sharing and Complaint Referral Arrangements are available on our website at www.lawlink.nsw.gov.au/privacynsw (via About us > Policies and Protocols).

The (commonwealth) Office of the Privacy Commissioner (OPC) and Privacy NSW have entered into a memorandum of understanding (MOU), which came into effect on 20 December 2005 for a period of two years. Both Commonwealth and NSW legislation cover health privacy issues so the OPC and Privacy NSW agreed to give individuals a choice as to the regulator they wish to approach in the first instance, and to ensure that generally health privacy complaints are only subject to investigation by one regulator.

If an individual wishes to lodge a privacy complaint against a NSW public sector agency or council, we will in most cases recommend that the person lodge an internal review directly with the agency or council. This approach provides the complainant with the option of taking the matter to the Administrative Decisions Tribunal (ADT) should they be unhappy with the outcome of the internal review.

The PPIP Act does not provide the option for a matter to be reviewed by the ADT after it has been investigated and conciliated by the NSW Privacy Commissioner. However, in certain circumstances, complainants may prefer to have their complaints against the NSW public sector investigated by Privacy NSW rather than by the agencies themselves.

A complaint about the handling of health information against a private sector person or organisation may be brought either to Privacy NSW or the commonwealth Office of the Privacy Commissioner (OPC).Complainants are given a choice, although it should be noted that the internal review option is not available, when a complaint is made against a private sector person or organisation.

When we decide to investigate a complaint, we also endeavour to resolve the complaint by conciliation. We seldom undertake a face-to-face conciliation but use correspondence. If the complaint is found to be valid we ensure that all parties to a complaint are aware of the issues. We also attempt to reach a conciliated settlement of the matter which would often involve the party complained about taking steps to protect privacy better in the future.

Complainants were first given the opportunity to lodge their privacy complaints directly with public sector agencies as internal reviews in the 2000-01 financial year. The internal review option has gained greater acceptance as a viable complaint mechanism with each subsequent year.

Internal review applications to public sector agencies

An internal review is an internal investigation that a NSW government agency is required to conduct when an individual makes a privacy complaint under Part 5 of the PPIP Act or Part 3 of the HRIP Act.

The Privacy Commissioner has an oversight role in the conduct of internal reviews. Privacy NSW must be notified by agencies of all internal review applications they receive and the Privacy Commissioner may make submissions to agencies on the procedural aspects of the review.

The oversight role of Privacy NSW

Agencies are increasingly inclined to treat complaints in the spirit in which they are intended rather than only referring a matter to internal review if a complainant makes a formal request for it. However, there is room for improvement as regards the manner in which agencies conduct internal reviews. The main areas where agencies require further guidance are:

- ensuring that Privacy NSW is notified when an application for internal review is received
- ensuring that internal review findings are reported to Privacy NSW before finalisation.

If an agency does not notify Privacy NSW of its receipt of an internal review in a timely manner, the Privacy Commissioner is denied an opportunity to make submissions to the agency in relation to the application, as is required under section 54(2) of the PPIP Act.

In some cases Privacy NSW has recommended that internal review findings be revised and reissued to the applicant because:

- the findings did not refer to the IPPs in any way and/or
- the findings did not make reference to the applicant's right to appeal to the ADT.

Examples of less significant comments made by Privacy NSW in regard to Internal reviews were:

- reminding the agency of the need to notify us of the lodgement of the Internal Review application
- reminding the agency of the need to make progress on the review.

Internal Review Case Studies

Disclosure of personal information in a public register

A NSW public sector agency that administers a public register received a complaint from an individual (D), who was concerned that their personal information was being disclosed on the register.

D received a letter from the agency informing D that information pertaining to D would be available on the public register and would be published on the internet. The agency proposed that the register would (amongst other things) contain D's name, sex, suburb and qualifications (this was usual practice). In D's case the register would also include certain other personal information that the agency believed it was legally obliged to put on the register.

D made an application under section 21 of the *Health Records and Information Privacy Act 2002* (HRIPA) to the agency for an internal review. D complained that D's health information would be disclosed to the public if the agency included the proposed extra information on the public register. In the application, D asked that the agency change its practice of making this sort of extra information available to the public.

In their findings the agency found that the information it was including on the public register did not amount to health information, as defined under section 6 of the HRIPA.

For completeness, the agency also considered the application from the perspective that the information was health information. The agency considered Health Privacy Principles (HPPs) 5,10 and 11. HPP 5 governs the way a person's health information should be stored by an organisation. It must be held securely and not longer than is necessary. HPP 10 limits an organisation's use of health and information. HPP 11 limits an organisation's ability to disclose health information.

In its findings, the agency referred to section 57 of the *Privacy and Personal Information Protection Act 1998* (PPIPA). This section gives an agency that is responsible for a public register the ability to disclose personal information in the register, if it is for a purpose relating to the register or the legislation under which the register was created. In this case, the agency was of the view that the register had been set up under legislation that required the agency to disclose the extra information in question.

The agency ultimately found that it did not breach D's privacy and was not prepared to alter its practices. The agency took the view that the public register operated lawfully and that it complied with relevant legislation.

Allegation of unlawful disclosure and inaccurate health information

W complained that under the *Health Records and Information Privacy Act 2002,* an agency had breached W's privacy on three separate grounds:

1. That confidential letters written by a specialist were improperly put on a hospital medical record. If confirmed this could constitute a breach of Health Privacy Principles 1, 2 and 3.

2. That inappropriate persons had been given unauthorised access to the health record. If confirmed this might constitute a breach of Health Privacy Principle 5.

3. That a health worker had recorded inaccurate information on the medical record and this might constitute a breach of a Health Privacy Principle.

The agency conducted a detailed Internal Review of W's complaint. It found that W had voluntarily enclosed the confidential letters from W's specialist with a referral to the hospital. Accordingly, there was no breach of a Health Privacy Principle. The Internal Review found that access to W's medical record was only afforded to those persons who had an entitlement to access, therefore, there was no breach of Health Privacy Principle 5.

The Internal Review found, however, that there may have been inaccurate and unnecessary notations made on the medical record by an employee in relation to a private conversation. Accordingly, there might have been a breach of Health Privacy Principle 9 which concerns accuracy of health information.

The Internal Review recommended no further action be taken in relation to complaints (1) and (2). However, in relation to complaint (3) the Internal Review recommended appropriate amendments be made to W's medical record and that the employee be relevantly counselled regarding the proper collection and entry of medical information.

Privacy NSW decided not to make any significant procedural submission regarding the Internal Review but advised the agency to inform W of their right to request a further review from the Administrative Decisions Tribunal.

Unlawful disclosure of health information

In this matter X requested that a NSW agency conduct an Internal Review.

X's child was attending a clinic for treatment of a disability. A NSW agency operates the clinic. At the relevant time, X's parent was the primary carer of X's child and attended the clinic with X's child.

The purpose of the Internal Review was to investigate a complaint by X that an unidentified person at the clinic improperly disclosed private and personal information relating to X's parent. This personal information had then been accessed by a government Department and used by that Department.

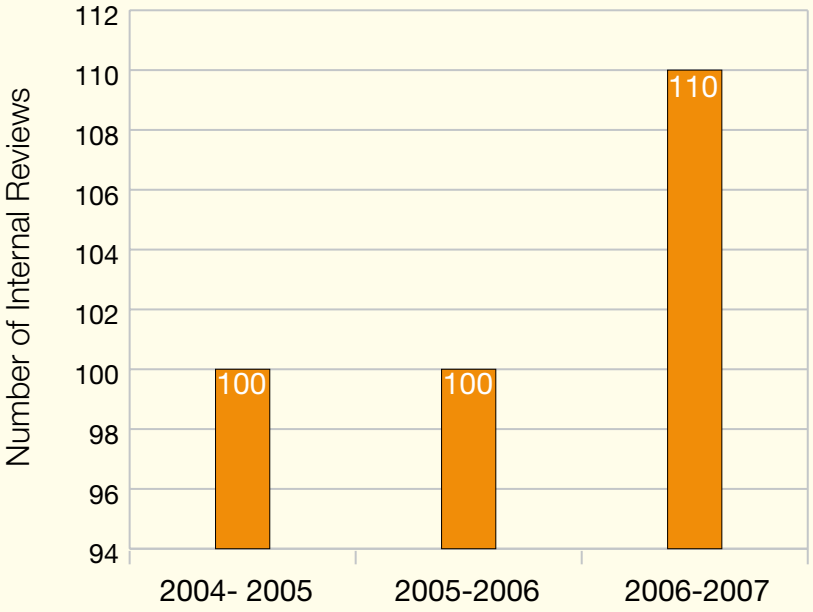
X sought an apology from the agency, withdrew their child from the clinic and sought compensation in the form of a contribution to the costs of X's parent in reversing the actions of the Department which relied on the information disclosed.

The agency commenced the Internal Review but prior to it concluding and reporting, X withdrew the complaint. The agency made an undertaking to conclude the Internal Review, prepare a report and forward a copy to Privacy NSW.

Allegation of unlawful access and use of personal information

T, a teacher at a school, was travelling by car late one evening. The car in which T was travelling nearly collided with another vehicle, which was being driven at high speed. The other vehicle then sped away. T, believing they recognised the vehicle, followed it. When the driver alighted from the other vehicle, T recognised a student from their school.

New Internal Reviews



T did not want to report the incident, as T felt it would have been unfair to the student. T determined instead to contact the student's parents directly and tell them what had happened, in the hope that they would encourage their child to drive more safely. On the weekend, T attempted to locate the student's home number in the telephone book. It was not listed. T then decided to drive to the school and access the school computer records and find the telephone number that way. T found the number and telephoned the student's parents on the weekend and told them about the incident.

The student's parents were displeased amongst other things because they had been contacted on the weekend and that T had accessed their unlisted telephone number from school records. One of the student's parents subsequently made a privacy complaint about T having accessed school records inappropriately.

The *Privacy and Personal Information Protection Act 1998* provides for the protection of personal information held by public sector agencies. T, as an employee, may be covered by the Act.

Personal Information is defined in section 4(1) of the Act as information or an opinion, whether or not recorded in a material form, about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. Section 4(3)(b) provides that personal information does not include information about an individual that is available in a publicly available publication.

As a result of the complaint, the agency in question undertook an internal review of the matter. The internal review looked at whether the student's home number was personal information and found that, though T had used the school records to access the student's telephone number, the number was available in various local publications. For this reason it was held not to be 'personal information'.

The internal review stated that, in the alternative, if the information was considered to be 'personal information' for the purposes of the Act there would arguably still not be a breach of the Act, as when the student had been enrolled at the school, his parents had signed the enrolment form with a 'Privacy Notice' and this allowed

personal information to be accessed for the purpose of 'communication with students, parents' and 'for other matters relating to the welfare of a student'. The agency was of the view that the accessing of the student's home telephone number from the school records was directly related to the welfare of the student and to the duty of care that it owed to the student.

Privacy NSW is not aware of any appeal to the ADT in this case.

Note

Agencies should be aware that in some circumstances the accessing of personal information might not constitute a breach of the Act, for example, where the information is already publicly available. Members of the public, however, may not be aware of these exceptions. For this reason Privacy NSW recommends that agencies ensure that their staff undertake privacy training and are made familiar with some of the more esoteric aspects of the NSW Privacy legislation.

Advice Case Studies

Obtaining client's consent to collect personal information

We had received a number of inquiries from Department of Housing tenants in relation to the Department's Application for Rental Subsidy and Rental Subsidy Renewal Certificate forms. The forms had to be completed by those seeking to apply or renew eligibility for the rental subsidy, which the Department provides to low-income tenants. Both forms request tenants' and other household members' financial and other information and also requested consent to the Department verifying the information provided with third parties. Some tenants found it confusing that what they considered to be two different matters i.e. (a) a declaration that the information provided is true and correct and (b) consent for verification of this information, were required to be verified by only one signature.

We assessed the forms and agreed, that tenants should have the option of making an application to renew their rental subsidy without at the same time consenting to the Department verifying the information from third parties. We then wrote to the Department inviting their representatives to a meeting about the issue and to discuss whether the forms might not be able to be redesigned.

In our opinion the best way to address the complainants' concerns was to redesign both forms so that tenants can provide 2 signatures: one to declare the accuracy of the information provided and another one to consent to that information being verified by the Department with third parties. Although we pointed out to the complainants that withholding their consent may result in their rental subsidy not being granted, many of our enquirers would prefer to have the choice of giving or withholding their consent (without that choice consent is not genuine). The meeting with the Department of Housing representatives was very productive. We had a look at the forms, explained to them best privacy practice in relation to consent and discussed the enquiriers' concerns. Our suggestions in relation to redesign of the forms were accepted by the Department and some time later we were provided by the Department with new forms that incorporated our suggestions in relation to the consent issue. We were also invited to make some suggestions as to wording and layout. The Department agreed to incorporate our suggestions in the next reprint of the forms.

Disclosure of council's credit card expenditure

Privacy NSW received a request for advice from Kempsey Shire Council regarding the disclosure of information about staff, which could be viewed as personal information.

Kempsey Shire Council received requests from members of the community to release details of the credit card expenditure of officers of the agency. The agency responded by making public a report outlining the names of the conferences attended, number of staff, who attended and the cost. Initially, the agency considered including the names of the staff members attending the conferences, but due to the concerns of staff members, the council did not include the names in the draft report.

The agency sought the advice of Privacy NSW as to whether they could include the names of staff in the publicly available report, without the consent of staff members. The council also sought advice from the two other legal advisers.

Kempsey Shire Council informed Privacy NSW that one source of legal advice supported the release of the names (or at least the position titles) of the staff attending conferences in their capacity as public sector officials. That legal advice viewed this approach as being consistent with the public interest and ensuring transparency in government decision-making.

Another source from which the Council took legal advice held the view that disclosure of staff names would be a breach of the *Privacy and Personal Information Protection Act 1998* (PPIP Act), specifically section 18.

Privacy NSW advised the council that it is not able to provide legal advice, in case it conflicts with the Commissioner's complaint handling function which requires him/her to take a neutral position in order to conciliate complaints. For the same reason Privacy NSW cannot adjudicate between differing legal views. Despite this, Privacy NSW provided the council with a few general observations.

NSW Electoral Commission and Easy Voting Card

In the lead up to the March 2007 New South Wales state election Privacy NSW received 7 complaints and enquiries in relation to a mail out by the NSW Electoral Commission of an elector brochure and easy voting card. The brochure contained general information about the election and the easy voting card, which formed part of the brochure, contained individual's enrolment details including their name, address, date of birth and the electoral district they belonged to.

The main privacy concern expressed by people who contacted us centred on their personal information, specifically their date of birth, being included in the mail out, along with their name and address. People were worried that this information might fall into the wrong hands and possibly give rise to identity theft. Complainants pointed to the danger of having their date of birth information provided in circumstances where the addressee has moved and the correspondence is then left unclaimed "for all to grab". The risk of the information being misused, when left unclaimed, may be much higher in large residential complexes.

Another example given was that some electors might mistake the electoral brochure for some sort of 'junk mail' and discard it without realising that their personal information, particularly their date of birth, is included with the brochure. Overall, the complainants expressed a view that inclusion of their date of birth with the brochure was potentially privacy intrusive and not necessary. Some of the complainants were further concerned about their dates of birth being freely available for public inspection as part of the electoral roll.

In considering the issue, we contacted the NSW Electoral Commission for their views. It turned out that the amendments made to the *Parliamentary Electorates and Elections Act 1912* (the PE&E Act) last year removed the requirement for electors to provide their occupation details and required them instead to provide their date of birth. The effect of the amendment is that electoral officials at the time

of voting are required to ask for a voter's date of birth to confirm their identity.

The NSW Electoral Commissioner (NSWEC) argued that the purpose of the easy voting card is two-fold: first, it draws an elector's attention to the details that are currently held by the NSWEC, giving them an opportunity to correct any mistakes, and secondly, it assists election officials to locate the elector on the certified list and reduces the time electors spend in line waiting to have their name marked off the roll on election day.

The Electoral Commissioner considers it necessary to provide certain important election information directly to each elector and is of the view that this does not constitute insensitivity regarding the elector's personal information nor a breach of an elector's privacy, given that, as far as the Electoral Commissioner was aware, the correspondence was individually addressed, posted in a sealed envelope and delivered by Australia Post.

We noted in our advice to the complainants that the PE&E Act provides strict guidelines as to how the rolls can be publicly inspected and prohibits disclosure or commercial use of enrolment information, placing heavy penalties on offenders. We appreciate that the discretion whether to provide dates of birth for public inspection rests with the Electoral Commissioner and we obtained assurances from the Commission that there is no intention to make this information public.

Scanning of driver's licence as proof of identity or ID when entering a club or pub.

Privacy NSW received a request for advice, after a person was asked to confirm their identity before being allowed to enter a NSW club. Staff of the club instructed the patron that their driver's licence must be presented, took possession of the licence and then scanned it. The information detailed on the licence was recorded on a compact disk.

The club had introduced scanning machines as an alternative to the manual sign-in method. The club does provide an option for manual sign-in but requires some proof of age (the sign-in is done directly onto touch screens). The sign-in slip has limited information on it and includes a file identifier. Access to this sign-in is limited to certain office staff in order to provide protection against loss of the sign-in slip and the patron's details.

As part of the manual sign-in system the signed slips were kept in storage for seven years. The club, however, felt that the data was more secure and more compact, when stored on a compact disk. It was club policy that access would only be granted to the disk to police and similar agencies.

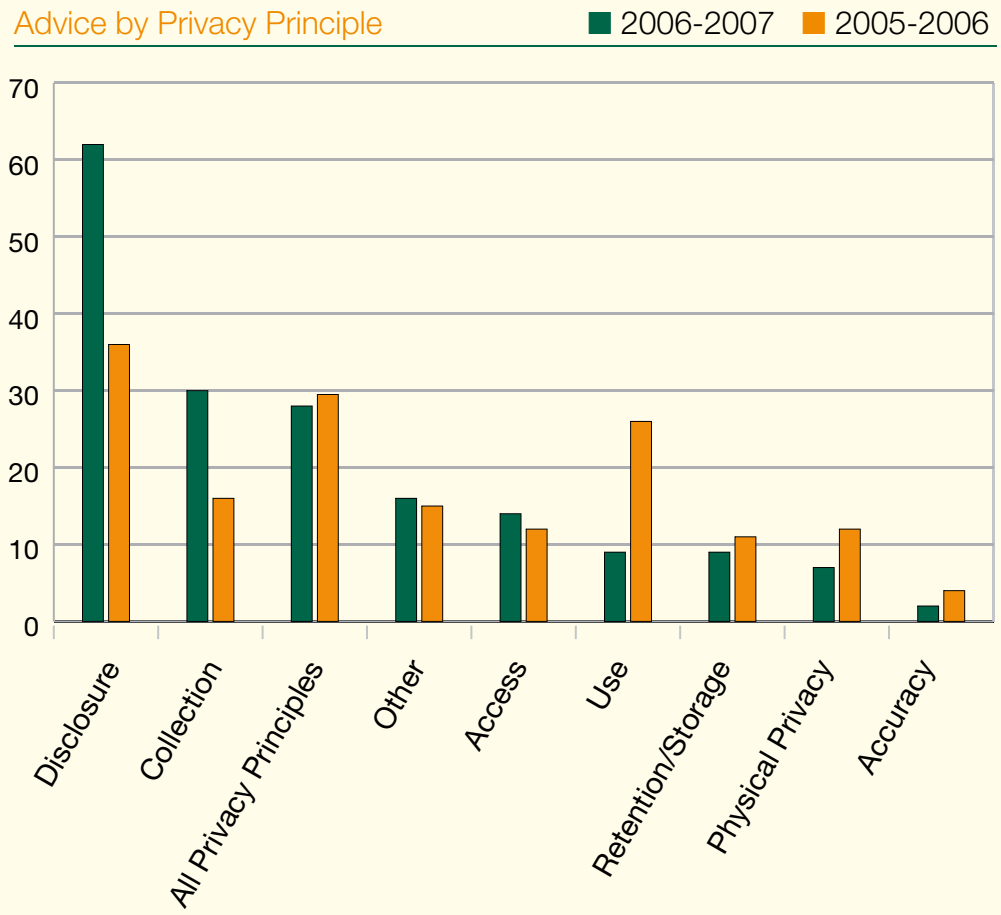
It was the club's view that patrons are responsible for placing their cards in the scanning machine in accordance with the *Registered Clubs Act 1976.*

The enquirer stated: *"None of this was pointed out to me, also the fact that I was being signed in by a member of the club, should have negated the requirement to provide a licence, also the Club Act only states that the name and address need to be kept in a register, not your licence and photo details".*

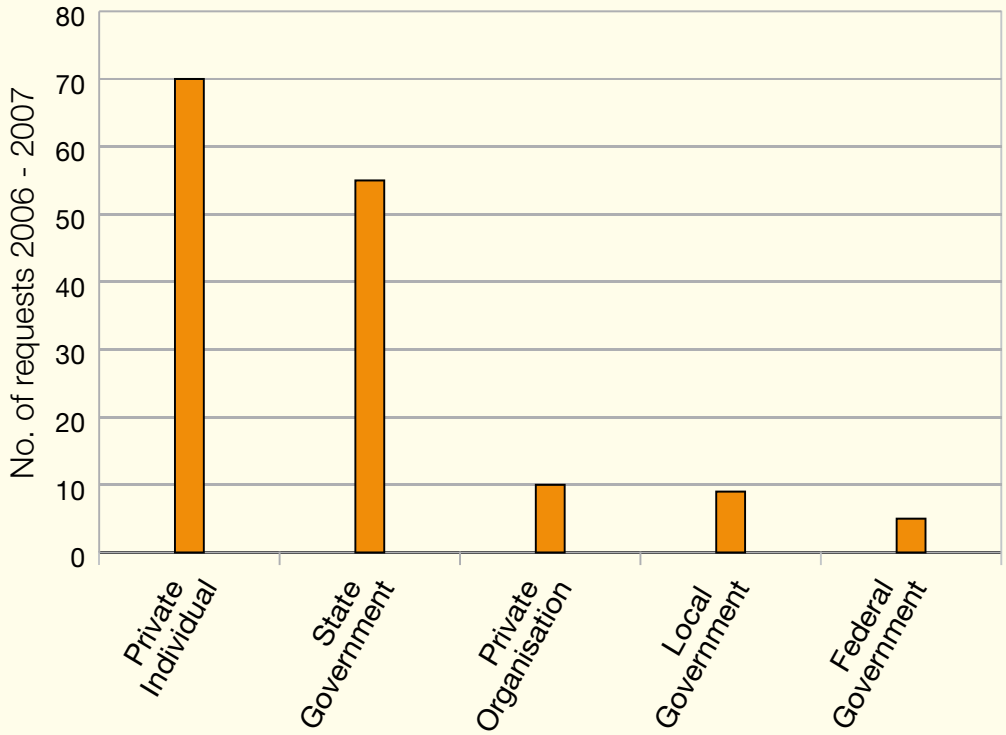
The enquirier was not so much concerned about the scanning of the licence but about what can be done with the (scanned) information on the licence, for example, copying of their signature. The information from the scanning process was to be stored for seven years in a fireproof safe.

The enquirer stated: *"These days, with the technology available and identity theft becoming more prevalent, ANYONE with access to this information, a computer, a "card" maker and the correct computer programs can become me (or you for that matter)".*

Advice by Privacy Principle



Main Sources of Request for Advice



Despite the club's privacy officer's assurance that replication of the complainant's details was not possible, the patron was able to demonstrate that it was possible.

The enquirier asked the privacy officer to view the licence data on the "relative" scanning program, take a "screen print" of what appeared and then paste this into to a word document. The result was a full copy of the licence including photo, signature and all other details on a word document. This document could be emailed, printed or faxed anywhere. The main concern was the fact that even the club's privacy officer did not realise this.

The Information Protection Principles in the the *Privacy and Personal Information Protection Act 1998* only apply to public sector agencies. Although clubs are registered under the *NSW Registered Clubs Act 1976,* they are private sector organisations and as such are more likely to be subject to the Commonwealth *Privacy Act 1988.*

Complaint Case Studies

Refusal to grant access to medical records

This is a case regarding access to medical records. In this case, a person (K) sought access to their medical records from a general practitioner. The general practitioner worked for a medical centre.

The medical centre refused to give the person access to their records under the *Health Records and Information Privacy Act 2002.* Privacy NSW advised the medical centre of its responsibilities. Unfortunately this had little effect and the medical centre still refused to release the records, although it offered to provide a written summary to the patient at a price.

Accordingly Privacy NSW issued a report to both parties to the complaint under section 47 of the *Health Records and Information Privacy Act.*

The issuing of a report enables a complainant to take the matter to the Administrative Decisions Tribunal (the Tribunal).

Note: The Commissioner has issued a number of such reports in the 2006-07 financial year, and in at least one case, the complainant has proceeded to the Tribunal and obtained access to their records.

Faulty Facsimile machine distributes health information

Privacy NSW (PNSW) received a complaint about the distribution of sensitive medical information.

The details listed below are a brief series of events both leading up to and after this incident occurred.

The complainant's spouse was issued with a medical certificate. This certificate was provided to the spouse's employer.

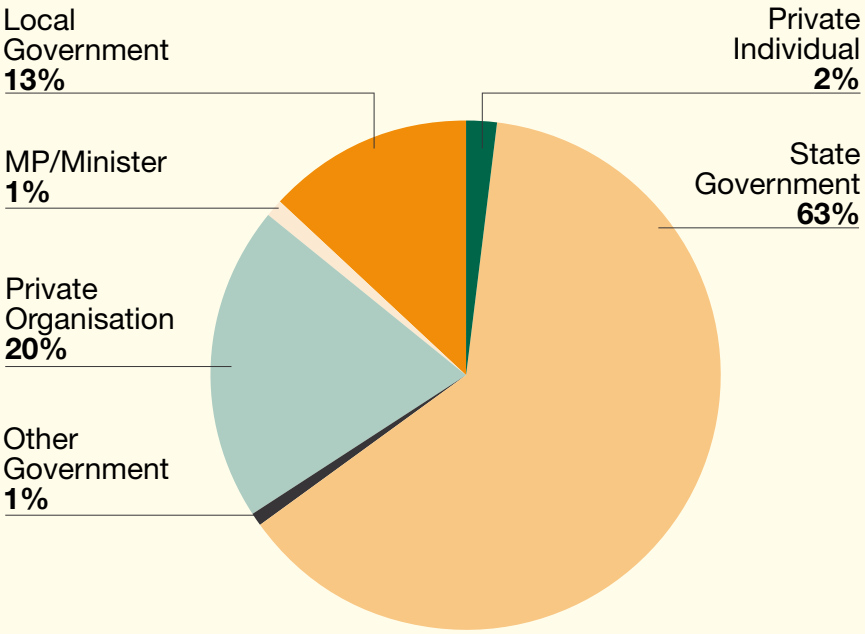
A day later the complainant received a phone call stating that a copy of these documents had arrived elsewhere in the organisation via the facsimile machine. The complainant then rang the area office and made enquires on how / why this document was sent to this location. Later that day the complainant was advised that the certificate had been faxed to various wrong locations. The agency also advised from that they were aware of the incident and were also checking on the complainant's welfare.

Later the organisation apologised for what had occurred and stated that there had been a machine malfunction.

The complainant was later advised that the fax machine had been tested and it appeared to have no faults.

The complainant found this unacceptable and wrote to PNSW seeking an investigation by an independent body and answers to how sensitive medical information has been distributed to

Main Sources of Request for Advice



potentially hundreds of staff of an agency when, apparently a fault with the fax machine was identifi ed some months previously. The complainant also requested that any action by the agency include a review of their procedures pertaining to the transfer of sensitive information.

In response to the complaint PNSW provided the complainant with detail about privacy law in NSW and the *Health Records and Information Privacy Act 2002* (the HRIP Act) in particular.

When the agency looked into the matter they determined that there had been a breach of the Health Privacy Principle 10 (use) and Health Privacy Principle 5 (retention and security) with regards to the health information. The agency also found that a copy of the certifi cate had, in fact, been sent to various locations of the agency in NSW. This was identifi ed as a "use" rather than a "disclosure" of the information as it was sent within the organisation. The review process included a service of the facsimile machine. The agency found that the machine was not functioning properly and this allowed the machine to transmit the information to random numbers stored in the machine. The machine was subsequently replaced.

The agency provided the complainant with an apology. The agency also made a recommendation that in future a fax cover sheet be used that clearly identifi ed the sender and the recipients and that the cover sheet include a disclaimer alerting unintended recipients to notify the sender if the fax was received in the wrong place and to destroy the document. The agency also added an automatic disclaimer to their email system to provide better protection for personal information.

An instructional circular was also to be issued to ensure that correct procedure was followed when sending a facsimile.

Disclosure of personal information to ministers of religion

Z was admitted to a hospital for a procedure.

Prior to the procedure he requested that hospital staff arrange for him to be visited by a minister of religion.

The hospital staff informed Z that the hospital no longer had visiting ministers of religion and that he would have to make personal arrangements for such a visit. It was said that to allow visiting ministers of religion might be in breach of privacy legislation.

Z complained to a Member of Parliament (MP) and the matter was referred to Privacy NSW. The NSW Privacy Commissioner informed the MP that there was nothing in privacy legislation to prevent a priest or other minister from visiting a hospital patient, if that patient so requested.

Loss of health information by a health service provider.

K complained to Privacy NSW that a health provider ("the Respondent") had lost K's medical file. The medical file contained sensitive personal information regarding K's past. Privacy NSW initially undertook research about the Respondent and confirmed that it was in receipt of state government funding, was subject to an annual audit by the NSW Auditor-General and, therefore, probably a "public sector agency" pursuant to the wide definition in Section 5 of the *Health Records and Information Privacy Act 2002* ("the HRIP Act").

Accordingly, under the HRIP Act, K could elect to pursue either an Internal Review of their complaint by the Respondent or an investigation / conciliation of the complaint by Privacy NSW. K elected to have the complaint investigated and conciliated by Privacy NSW.

Privacy NSW liaised with the Respondent, who then performed a thorough investigation of the substance of K's complaint and a review of office protocols and procedures regarding the proper security of K's medical files. The Respondent subsequently prepared a report of the results of its investigation and found that it had been in breach of Health Privacy Principle 5(1) (c) which requires that health information be protected by taking reasonable security safeguards against loss, unauthorised access, modification or disclosure.

K felt genuine upset and trauma at the loss of the medical file but was not seeking any financial compensation. What K sought was for the Respondent to make a written apology, give a written undertaking that the system for retaining and securing medical files would be improved and that staff would be given further training in relation to their responsibilities under the HRIP Act, in particular those relating to the use and disclosure of medical information.

Privacy NSW discussed these issues with the Respondent and after a short period of negotiation the Respondent agreed to all K's requests. The Respondent forwarded a formal, written apology and undertaking to K, the complaint was resolved and Privacy NSW closed the file.

Access as Executor

T contacted Privacy NSW with a complaint regarding access to T's deceased parent's health records. T's parent had been a resident at an Aged Care facility for a number of years before their death, and T, as executor of the Estate, was seeking access to a file.

T sent three written requests to the facility asking for a copy of the file. T received a response to the first request, which informed T that the request was being refused. T received no response to the following two letters. T then made a complaint to Privacy NSW alleging a breach of the *Health Records and Information Privacy Act 2002* (the HRIP Act).

Both the HRIP Act and the *Privacy Act 1988* (Cth.) deal with health information and the private sector. Part 4 of the HRIP Act deals specifically with the application of the Health Privacy Principles to private sector persons such as medical practitioners, private hospitals and nursing homes. The complainant chose to ask Privacy NSW to handle their complaint.

Section 8 of the HRIP Act allows for an 'authorised representative' to make a decision on behalf of another person, for example, to request their medical records under Part 4 of the HRIP Act. The 'authorised representative' can be someone who is authorised by law to act for or represent another person, such as, an executor on administration of a deceased estate.

By virtue of Section 27 of the HRIP Act, a private sector person must respond to a request for access within 45 days, and must provide a reason for any refusal of access.

Privacy NSW wrote to the Aged Care facility in question, on behalf of T, and explained to the facility its obligations under the HRIP Act. Upon receipt of the letter the facility granted T access to the file. If the facility had continued to refuse T access to the file, the Privacy Commissioner could have elected to prepare a report under Section 47 of the HRIP Act which would have outlined any of the Commissioner's findings or recommendations in regard to this matter and allowed the complainant to take their complaint to the Administrative Decisions Tribunal. This instance was an example, however, of the effectiveness of a conciliatory intervention by Privacy NSW and amounted to merely reminding an organisation of its obligations under the Act.

Emerging Issue

Access to court information

In the middle of last year we were asked by the NSW Attorney General's Department to provide our comments on a proposed review of the Department's policy on allowing access to court documents and information.

The aim of the review is to articulate a comprehensive policy on the subject of giving access to court information. A number of principles are involved. These include open justice, the protection of vulnerable persons involved in court proceedings and the recognition of the privacy considerations that might attach to certain information. The aim of the review is also to provide a framework for a uniform approach to the issue across all NSW courts.

We expressed our "in-principle" support for the proposal and suggested that we would like the review to achieve a balance between the proper administration of justice and individuals' rights to privacy, irrespective of whether these rights belong to the parties to the proceedings, their relatives or interested non-parties e.g. witnesses, etc.

We then shared our experience in this area, which is that the majority of privacy complaints received in relation to court documents, can be broadly divided into two categories: (a) complaints by relatives of a guilty party complaining of being victimised by association and b) complaints by witnesses, etc. that they are being harassed by the accused. There is also the well-known (albeit not as widely complained about) danger of victims of crime being embarrassed and victimised more, when their identity becomes public knowledge.

We opposed a proposal that all documents declared "open access" be made available to the media and to members of the public without those seeking access having to show sufficient cause. We expressed a view that there seems to be a trend towards allowing greater access to court documents, regardless of whether the interest of those seeking access is anything more than sheer curiosity.

We also suggested the review should provide further clarification as to what is to be made freely available on the Internet and whether there are plans for all "open access" documents to be made available on the Internet and, therefore, accessible to the general public. We indicated the dangers associated with having all accessible information available electronically. These dangers include magnified results of any errors, the unfairness of a selective reading, secondary uses of personal information, personal safety risks, identity theft and the difficulties involved in correcting mistakes.

In particular, we were concerned that litigants - particularly unrepresented litigants - may not be aware of their right to ask a court to suppress their identity and/or other personal information. We suggested the new uniform court rules and forms make this right clear, preferably by stating it in bold on court documents. As regards any future Internet access policy, we alerted those doing the review to the US experience in this area. We generally agree with the recommendations for courts to take a "go-slow" approach to posting public records on the Internet and to use a "two-tier" access policy when appropriate. This view was expressed in a US article "Public Records on the Internet: The Privacy Dilemma", which can be found using the following link: http://www.privacyrights.org/ar/onlinepubrecs.htm

We understand that the new policy on access to court documents is being developed and are hopeful that some of our recommendations will be implemented.

Applications to the Administrative Decisions Tribunal

If a person, who has requested an agency to conduct an internal review, is not satisfied with the outcome of the internal review, or if the agency takes longer than 60 days to complete the internal review, the complainant can apply to the Administrative Decisions Tribunal (the Tribunal) for a review of the agency's conduct.

The Tribunal can review conduct that allegedly breaches an Information Protection Principle (IPP) under the *Privacy and Personal Information Protection Act 1998* (the PPIP Act) or a Health Privacy Principle (HPP) under the *Health Records and Information Privacy Act 2002* (the HRIP Act). If the Tribunal finds that an agency has breached one of these provisions, it can make enforceable orders against the agency.

In certain circumstances the Tribunal can make inquiries into complaints against private sector persons. This is possible under section 48 of the HRIP Act but only if the complaint was the subject of a report of the Privacy Commissioner, which was furnished to the parties to the complaint (section 47).

In the 2006-07 reporting year, Privacy NSW increased its participation in matters before the Administrative Decisions Tribunal. Currently, we endeavour to attend at least one planning meeting for every new privacy matter.

What follows is an extract from a talk given by the Privacy Services Manager to the Risk Management Institute of Australia in August 2007.

There have been a number of significant decisions in the area of privacy this year. One of the most significant, in that it deals with the issue of damages, is the decision in *JD v New South Wales Medical Board (No.2) [2006] NSWADT 345.* This case is important because the applicant was awarded $7,500 in damages. This is the highest amount of damages we are aware of in a Tribunal privacy decision, although in *GR v Department of Housing (No 2) [2005] NSWADT 301* Judicial Member Robinson stated, "I would have ordered the respondent to pay the applicant a sum that took the total amount to $15,000" .

It would appear, therefore, that the amount of damages awarded by the Tribunal is going up, although it remains far less than most common law damages, defamation awards or what many privacy complainants would like to receive.

Prior to this case, which dealt primarily with how much JD should be awarded, the Tribunal had found that the New South Wales Medical Board breached sections 18 and 19 of the PPIP Act by disclosing JD's health information contained in a psychiatric report (the report was included with the Medical Board's determination).

In this case, Judicial Member Montgomery noted, that in privacy matters in the Tribunal, the successful party does not always receive damages. The Tribunal quoted its President in *NW v New South Wales Five Brigades (No.2) [2006] NSWADT 61* at [23]:

"In my view the award of statutory damages in Privacy Act matters remains a discretionary one even where a causal link sufficient to satisfy section 55 (4)" [exists]. "That the position under the statute is less automatic is reflected, I consider in the language of the opening words of section 55 (2):

'On reviewing the conduct of the public sector agency concerned, the Tribunal may decide not to take any action on the matter. Or it may make one or more of the following orders....'

These words do not preclude the possibility that the Tribunal might find the contravention, might find a causal link between the contravention and harm suffered and make no order…" (sc. for damages).

Despite quoting these remarks, the Tribunal awarded JD damages of $7,500, which were meant, in accordance with the traditional legal principle, to restore the applicant (as much as money can do) to the position he would have been in, had his privacy not been breached. The Tribunal did not, however, award many of the other things JD claimed. It did not award anything for the financial loss he suffered in not being able to find employment. It did not award anything as recompense for his medical costs. It did not order that the apology given by the Medical Board be made public. It did not award JD his costs for attending a psychiatrist and it did not award the costs of his psychiatric witness attending court.

There were two principles behind the Tribunal not awarding the other matters claimed by JD. One was that the applicant did not put sufficient evidence before the Tribunal as to some of the costs he had incurred, for example, his financial loss from being unemployed. It is true that the applicant advanced a round figure but clearly the Tribunal, as is its usual practice, requires more detailed evidence than that. In the case of JD being unemployed, perhaps a statement by an actuary or estimate on the basis of his previous tax returns might have been helpful.

As regards some of the other matters the applicant claimed, the Tribunal felt there was not a sufficient causal link between the privacy breach and what was claimed. For example, the Tribunal was of the view that the applicant was obliged to attend a psychiatrist regularly for other reasons. This was why it did not award him those costs.

It is possible for the Tribunal to make awards for costs against a respondent in "special circumstances" and this matter was considered by the Tribunal in relation to the witness expenses of JD. The test for making such an award is, however, very demanding and was not met in this case.

VA v Director General, Premier's Department of New South Wales [2006] NSWADT 249 demonstrates that, if an internal review is carried out thoroughly and there is no evidence of a breach of privacy, that internal review is likely to be upheld by the Tribunal.

That, at any rate, was the result in VA's case. Premier's Department carried out a particularly thorough internal review, after initially misplacing the applicant's request for it. In their review, Premier's Department found no evidence that either DADHC or the responsible Minister's office had disclosed the personal information of the applicant in breach of either sections 18 or 19 of the PPIP Act.

In this case, VA claimed that his personal/health information had been given to a journalist by either staff of DADHC or the responsible Minister, at a time when the applicant was to be interviewed about his request to maintain the level of his disability services (his case had been the subject of a question in Parliament).

In their review, the Tribunal upheld the finding of Premier's Department, which undertook the internal review on behalf of DADHC and the Minister's office. The Tribunal was of the view that there were other possible sources for the leak to the journalist. In addition, the Tribunal applied the recent, highly significant decision of *Macquarie University v F M [2005] NSWCA 192*, which, amongst other things, held that verbal information or opinions of an agency's staff cannot be "held" by the agency for the purposes of the PPIP Act, if the opinions and information are not in written form. In this case, there was no documentary evidence of the material alleged to have been disclosed and hence the Department could not have "held" it for the purposes of section 18 (the disclosure provision). Consequently there was no breach of the PPIP Act and the Tribunal had no jurisdiction.

As regards the alleged breach of section 19 (relating to disclosure of sensitive information),

What is Privacy NSW's role in the Administrative Decisions Tribunal?

Privacy NSW is notified of applications to the Administrative Decisions Tribunal and has a right to appear and be heard in privacy matters before the Tribunal. The Privacy Commissioner is usually represented by one of Privacy NSW's officers.

Our role in the Tribunal is primarily concerned with assisting the Tribunal in interpreting the PPIP Act and, more recently, the HRIP Act. In accordance with the Commissioner's various functions relating to the protection of privacy, we are concerned that the PPIP Act and the HRIP Act are interpreted in a way that promotes the objects of the Acts.

Our role in the Tribunal is not about supporting, or advocating for, either the applicant or respondent. However we may provide limited assistance or information to parties in relation to substantive or procedural issues arising under the PPIP Act and the HRIP Act.

Further, in view of the Privacy Commission's role as a conciliation agency, the Commissioner or his representative will provide whatever assistance they can to the Tribunal to bring about an appropriate settlement of the matter during the planning or hearing stages.

the Tribunal simply held there was not sufficient evidence to establish any conduct or "alleged conduct" for the Tribunal to review (section 55).

A "hot" issue in recent Tribunal cases has been the width of the exclusion from the definition of personal information at PPIPA, section 4 (3) (j) ("information or an opinion about an individual's suitability for appointment or employment as a public sector official"). In this respect *Department of Education and Training v PN (GD) [2006] NSWADTAP 66* is a significant decision. This was an appeal heard by the Appeal Panel of the Tribunal from a decision made by Judicial Member Montgomery *(PN v Department of Education and Training [2006] NSWADT 122).* In that case PN, a teacher, alleged certain breaches of their privacy made by various staff of the Department in the context of a workers compensation claim and subsequent return to work program. The information dealt, among other things, with PN's co-operativeness, ability to work effectively as part of a team and interpersonal skills. The Department contended that all the information touched upon the issue of PN's employment with the Department and was thus excluded from the definition of "personal information" by virtue of section 4(3)(j) of the PPIP Act.

Judicial Member Montgomery analysed previous decisions made on this issue, including *Y -v- Director General, Department of Education & Training [2001] NSWADT 149,* decided by the Tribunal's President; *GL v Director General, Department of Education & Training [2003] NSWADT 166* and *EG v Commissioner of Police, New South Wales Police Service [2003] NSWADT 150* decided by the Deputy President. Judicial Member Montgomery noted [at 56] that the question as to whether or not information is "about an individual's suitability for appointment or employment as a public sector official" is to be determined by consideration of both the content and the context of the information. The Privacy Act is beneficial legislation and any exclusion from the definition of "personal information" should be interpreted narrowly [at 58]. Judicial Member Montgomery did not agree with the Department's contention that all information

touching upon the issue of PN's employment with the Department is necessarily information about PN's suitability for employment: "Taken to its logical conclusion would mean that even the most vindictive gossip about an individual could attract exclusion under section 4(3)(j) of the Privacy Act. This is inconsistent with the protection of the privacy of individuals generally and in my view could not have been the intention of the legislature." The Member concluded at first instance that the information at the heart of the complaint was personal information; that it was not excluded from the operation of the legislation and that the Tribunal had jurisdiction to hear and determine the matter.

The Department then appealed this decision to the Appeal Panel of the Tribunal. The Appeal Panel consisted of three Judicial Members. The decision of the Appeal Panel thoroughly analysed six previous decisions of the Tribunal on this issue. The Panel upheld the decision of Judicial Member Montgomery and made the following concluding observations [at 78]: "Our opinion of the true construction of s 4(3)(j), based as it is on prior decisions of the Tribunal, attributes to it a narrow scope of operation…As we see it, the difficulties of interpretation posed by this legislation require close attention both to the precise nature and content of the information to which the proceedings relate and the precise context or contexts in which it is 'collected' by the relevant agency."

Development Applications to Local Council

Local Councils placing personal information on Development Applications on the Internet

A number of enquiries about Councils placing personal information on the internet prompted the Acting Privacy Commissioner to place the following advice in the 'What's New" section of Privacy NSW's website on 5 December 2006:

"Privacy NSW is aware that there are differing legal views as to whether Local Councils are able to put Development Applications and associated materials on the Internet. In those circumstances, I strongly advise Local Councils to take legal advice before placing such material on the Internet, and suggest it would be more prudent not to do so. In addition, if such materials are placed on the Internet via a website, I suggest Councils remove or black out personal information such as signatures and names/addresses of third parties. The appearance of signatures etc. on the Internet could assist identity fraud.

Privacy NSW has had a number of formal and informal complaints on this subject. It is suggested that members of the public, who want personal information of this kind removed by a Council, approach the Council in writing (we are aware that Councils have removed material when asked). If this does not work, members of the public can ask the Council to undertake an internal review about the matter under the PPIP Act or make a complaint to Privacy NSW (Ph: 02 8688 8585). Information about making a privacy complaint is available on this website.

Note: The interaction of privacy, local government and freedom of information legislation is complex and legally controversial. Privacy NSW will be making a submission to the NSW Law Reform Commission that this area be clarified".

PPIP Act Online Training Program

Privacy and Personal Information Protection Act 1998 Training Program – an interactive on-line program

The *Privacy and Personal Information Protection Act 1998* Training Program was initially developed as an interactive CD in 2002-03 by the NSW Department of Commerce and Privacy NSW.

In November 2006 PNSW offered an on-line training program for the *Privacy and Personal Information Protection Act 1998* to replace the CD application. The new on-line training Program (PTP) was updated to reflect recent changes in, and to the interpretation of NSW privacy legislation. The on-line program aims to help State government employees to comply with the *Privacy and Personal Information Protection Act 1998* (PPIP Act). It is operated for Privacy NSW by a website host with Privacy NSW paying a fee for the service.

The program provides training in the operation of the PPIP Act, enabling those who participate to test their understanding and work at their own pace. The program is highly interactive with periodic user testing and:

- provides bookmarking, which allows users to begin from the same point at the next session;
- allows users to record comments; and
- prints a certificate of achievement for users who complete the course.

In May 2007 in conjunction with the program website host, further refinements were made to allow the program to be accessed by agencies using recently introduced search engines. The program has attracted interest and will be monitored for usage during the coming year.

At the moment, due to the cost of the maintaining the Program, potential users must contact Privacy NSW to be given access.

IPART Investigation

Participation in the Independent Pricing and Regulatory Tribunal's (IPART's) Investigation into the Burden of Regulation in New South Wales and Improving Regulatory Efficiency (Working Group on Privacy)

Privacy NSW was approached by the Independent Pricing and Regulatory Tribunal (IPART) for comments on whether privacy regulation and non-disclosure protections may be imposing an 'unnecessary' regulatory burden on business or government in restricting information-sharing amongst government agencies. This was a concern raised in submissions to IPART's *Investigation into the Burden of Regulation in New South Wales and Improving Regulatory Efficiency.* IPART convened a Working Group on Privacy to further examine this issue.

We made some general comments focussing, in particular, on the need for more education about privacy and the common tendency to blame privacy legislation for things that were not in fact regulated or even prohibited by privacy legislation.

A representative of Privacy New South Wales was subsequently invited to a meeting of the Working Group, at which issues of concern were discussed. At that meeting, amongst other things, a number of legal issues were clarified, which had been raised by those making submissions to the Investigation by IPART.

Members of the Working Group were provided with a draft research paper for comment. Amongst others, Privacy New South Wales had the opportunity to contribute to this draft paper, which was subsequently released as part of IPART's Draft Report. The Draft Report is presently available on the IPART web site and the closing date for submissions was the 18th of August 2006.

From the point of view of privacy in New South Wales, some of the most important items in the Draft Report were the following:

- It was established that non-disclosure provisions were to be found in individual legislation administered by relevant agencies, as well as in privacy legislation.
- Privacy New South Wales emphasised that the state's privacy regulation is not restrictive provided agencies secured an individual's " informed consent".
- It was noted that privacy legislation does not regulate non-personal business information, such as company and most business names and addresses.
- Privacy New South Wales was able to advise that improvements have been made in the length of time taken to obtain an exemption under privacy legislation. Although, as those who made submissions complained, seeking an exemption can sometimes involve a lengthy process, urgent exemptions approved by the Privacy Commissioner can be made in a matter of weeks.

The Draft Report also contains discussion of the joint state and Commonwealth regime covering health information privacy and its attendant difficulties.

Amongst the other recommendations in the Draft Report, the Tribunal made the following important recommendations that relate to privacy:

- Privacy New South Wales and possibly the New South Wales Crown Solicitor could play an important advisory role in helping agencies identify options for improving information sharing in a manner that balances privacy protection with efficiency gains.

- that an interagency working group of senior officers (including representatives from Privacy New South Wales) be convened to identify further opportunities where it would be appropriate to share or streamline information among government agencies.

- that the government provide guidance to agencies on privacy requirements affecting information sharing between agencies.

PrivacyNSW would like to thank IPART for the opportunity to participate in the Working Group and contribute to the Draft Report.

Privacy Law Reform

- National, State and across the Tasman.

The review of privacy law at both a National and State level proceeded further in 2006 -2007 following the release of the Terms of Reference in early 2006 by the Australian and New South Wales Attorneys General.

At a national level the Australian Attorney General asked the *Australian Law Reform Commission* to examine the *Privacy Act 1988* and report any recommended changes by March 2008. The New South Wales Attorney General asked for a similar review of privacy and related legislation in New South Wales, including whether there should be a statutory tort of privacy.

On 11 April 2006, the NSW Attorney General, the Hon R J Debus MP made the following reference to the NSW Law Reform Commission:

Pursuant to section 10 of the *Law Reform Commission Act 1967* (NSW), the Law Reform Commission is to inquire into and report on whether existing legislation in New South Wales provides an effective framework for the protection of the privacy of an individual. In undertaking this review, the Commission is to consider in particular:

- The desirability of privacy protection principles being uniform across Australia;

- The desirability of a consistent legislative approach to privacy in the *Privacy and Personal Information Protection Act 1998*, the *Health Records and Information Privacy Act 2002*, the *State Records Act*1998, the *Freedom of Information Act 1989* and the *Local Government Act 1993*.

- The desirability of introducing a statutory tort of privacy in New South Wales.

- Any related matters.

The Commission should liaise with the Australian Law Reform Commission which is reviewing the *Privacy Act 1988* (Cth), as well as with other relevant Commonwealth, State and Territory agencies.

Placing the reform before the public - Public Meeting on Privacy and You

The New South Wales Law Reform Commission held a public seminar on the 26 March 2007 on a person's right to privacy as part of Law Week 2007 celebrations. All interested members of the public and legal profession were invited to attend.

The seminar focussed on whether a person should be able to bring an action to protect his or her privacy. The Chairman of the Law Reform Commission, Hon James Wood AO QC, said: "This law week seminar will highlight some of the complex issues in the law of privacy and consider whether the current law provides an effective framework for the protection of an individual's privacy.

We welcome input from interested members of the public on this topic. The seminar will provide an interactive, stimulating and informed learning environment for everyone present".

Professor Michael Tilbury, Commissioner in Charge of the NSW Law Reform Commission's review of privacy laws, outlined the scope of the privacy review. Attendees were invited to ask questions and raise issues.

Speakers included also NSW Law Professor Les McCrimmon, Commissioner-in-Charge of ALRC Privacy Inquiry.

Any member of the public can comment on the matters raised in the papers on privacy issued by the NSW Law Reform Commission. Submissions can be made in writing, or over the telephone to:

New South Wales Law Reform Commission
GPO Box 5199
SYDNEY NSW 2001 AUSTRALIA

The Australian Law Reform Commission also held a Privacy Inquiry Public Meeting on Thursday 15 March 2007 for small, medium and large businesses, employees and customers. It considered where privacy laws are working well and where they could be improved. Questions that the attendees were asked to consider included:

- Should employee records be covered by the *Privacy Act 1988* (Cth)?
- Are privacy laws stopping you doing business?
- Do privacy laws promote good business practices?
- Should small business be subject to the same privacy rules as large business?
- What rules should apply to personal information that is sent overseas?
- Do privacy laws impose an unwarranted compliance burden on business?

Presentations were provided by Professor Les McCrimmon, Commissioner-in-Charge of the ALRC Privacy Inquiry; Mr Malcolm Crompton, Managing Director, Information Integrity Solutions Pty Ltd and former Commonwealth Privacy Commissioner and Professor Michael Tilbury, Commissioner-in-Charge of NSWLRC Privacy Inquiry.

"There is ... a desperate need for one set of privacy principles, simply set out so that they can be easily understood. We ask the Commission to make this a priority in its recommendations".

Extract from the Submission by Privacy NSW in response to the Review of Privacy Issues Paper of the Australian Law Reform Commission February 2007.

Premier's Guidelines on Privacy & Industrial Relations

In June 2007 the Director General of the Premier's Department, Dr Robyn Kruk issued Privacy Guidelines on Disclosure of Information During Industrial Consultations in the form of a circular to all NSW public sector Chief Executives.

The Guidelines were based on previous Guidelines relating to the management of personal information by public sector agencies during industrial relations consultations. The new Guidelines incorporate advice about the requirements of the *Health Records and Information Privacy Act 2002* NSW (HRIP Act) in relation to health information and discuss the interaction between the requirements of the HRIP Act and the PPIP Act in the context of Industrial Relations and Occupational Health and Safety law.

The aim of the Guidelines is to assist agencies in making decisions about whether they can disclose personal information or health information to unions, where the authorised representatives of those unions seek to exercise their powers under the *Industrial Relations Act 1996* NSW or the *Occupational Health & Safety Act 2000* NSW. The Guidelines include a checklist of considerations that public sector agencies should take into account, before disclosing information.

The Guidelines also provide some guidance on the circumstances in which information about NSW public sector employees may be transferred to another public sector agency under the *Public Sector Employment and Management (General) Regulation 1996* NSW, for example where the disclosure of the information is necessary for inclusion in disciplinary and selection committee reports.

Privacy Awareness Week:

27 August - 2 September 2006

Privacy Awareness Week 2006 – educating the community

Privacy Awareness Week is an annual event aimed at raising awareness of the importance of protecting privacy. Privacy Awareness Week 2006 was held from 27 August to 2 September 2006 and was launched by the Commonwealth Attorney General, the Hon Philip Ruddock. Privacy NSW also launched some initiatives to mark this important week. The theme for this Privacy Awareness Week was "Don't leave privacy to chance" and a promotional poster was developed in conjunction with other privacy agencies in Australia (see picture).

Privacy Commissioners from Australia, New Zealand, Hong Kong, New South Wales, Victoria, Northern Territory and their organisations took part. Queensland, South Australia and Western Australia were also involved in Privacy Awareness Week.

Privacy Awareness Week 2007 – goes International

In April 2007 it was announced that this year, for the first time, Privacy Awareness Week would go international and would be jointly promoted by the Asia Pacific Privacy Authorities (APPA) forum members which included:

- Office of the Privacy Commissioner, Australia
- Office of the Privacy Commissioner, New Zealand
- Office of the Privacy Commissioner for Personal Data, Hong Kong
- Korean Information Security Agency
- Privacy Victoria
- Privacy NSW
- Office of the Information Commissioner, Northern Territory

The event would be highlighted in Australia, New Zealand and in Hong Kong. Privacy Awareness Week would begin on 26 August and conclude on 2 September and the theme for this year would be Privacy is Your Business.

In conjunction with the Privacy Awareness Week (PAW), the Asia Pacific Privacy Authorities launched an international privacy competition and have encouraged secondary school students to enter and to express their views on the relevance of privacy in today's society. Prizes offered include a laptop computer and gift vouchers.

APPA Network

The Asia Pacific Privacy Authorities meet twice each year to discuss contentious privacy issues arising in Australia, New Zealand, Hong Kong, Canada and Korea.

The network grew from informal meetings between Privacy and Information Commissioners from Australia and New Zealand during the nineties.

The emphasis at these meetings is on reviewing privacy issues which are emerging or causing concern in the countries taking part. The participating jurisdictions are made aware of different approaches which are being used to resolve privacy issues or to promote the concept of privacy.

During the two meetings of APPA this year – in Hong Kong and in Cairns – the participating agencies reached new levels of cooperation.

Agencies believe that there would be much to be gained by harmonising terminology and statistics. It would allow a better comparison of the privacy issues which arise and how the different jurisdictions deal with them.

The meeting in Hong Kong in November 2006 authorised Professor Paul Roth of the Faculty of Law, University of Otago, Dunedin, New Zealand to comment on the gathering of statistics, particularly those which appeared in Annual Reports of the agencies. The Commissioners also agreed that their Annual Reports would be submitted to a group of privacy and statistical experts to see how information presented in the Reports could be improved and harmonised.

The recommendations detailed in a Report prepared by Professor Roth, were considered at the (next) meeting in Cairns and many of his suggestions were adopted. Changes in the way the statistics have been presented in this Report reflect the comments and recommendations which have been made by Professor Roth.

Commissioners at the Hong Kong meeting in 2006 also attended informative sessions dealing with the use of closed circuit television and privacy training within large organisations.

The meeting in Cairns 2007 heard reports from the Australian Law Reform Commission, the New South Wales Law Reform Commission and the New Zealand Law Reform Commission concerning the references on the reform of privacy law.

At the conclusion of the meeting in Cairns the Commissioners authorised the release of the following communiqué summarising the discussions.

APPA Network: Further Discussions at the APPA Cairns Forum

Asia Pacifi c Privacy Authorities discuss initiatives in Cairns

27th Asia Pacifi c Privacy Authorities Forum 22-23 June 2007 Cairns, Australia Communiqué

The 27th Asia Pacifi c Privacy Authorities (APPA) Forum was held in Cairns, Australia on Friday 22 and Saturday 23 June 2007. The Forum immediately preceded the APEC Senior Offi cials Meeting and Seminar in Cairns, allowing participants to attend both events.

In attendance were the Privacy Commissioners and representatives of Australia, Canada, Hong Kong, Korea, New South Wales, New Zealand, Northern Territory and Victoria. Representatives from privacy related authorities in other jurisdictions also attended, including those from Mexico, the Australian Capital Territory, Queensland, South Australia, and Western Australia.

APPA has the principal objectives of:

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

Membership

APPA is pleased to announce that during the two day meeting in Cairns, 2007 it broadened its membership from seven authorities to eight, welcoming the Information and Privacy Commissioner of British Columbia.

APPA Forum Cairns: Program

The Cairns Forum saw jurisdictional reports delivered by member authorities and sessions on privacy-related developments in various countries. In addition to the Australian and New Zealand Law Reform references mentioned above, sessions included presentations on the Queensland smartcard driver's licence, biometric privacy concerns, internet leakage, a statutory cause of action for privacy and anti-money laundering.

APEC

APPA discussed the cross border enforcement aspects of the APEC Privacy Framework and the potential role for APPA and its members in the implementation of the Framework. The Forum also heard about similar cross border developments in the OECD.

Privacy Awareness Week

The APPA-wide youth writing competition and the presentation to the winner to coincide with Privacy Awareness Week in the last week of August 2007, was a focus of much discussion at the APPA Forum in Cairns. The Privacy Commissioners noted the warm relationship that had developed between the project's coordinators in the participating countries and the increased cooperative approach between the privacy authorities that resulted. It was noted that the sharing of resources had achieved more in promoting awareness of privacy rights than would have resulted had each data protection authority undertaken the project independently.

Biometrics Working Party established by APPA Forum in Cairns

Hong Kong, New Zealand, Australia, New South Wales, Victoria and the ACT agreed to establish a Working Party to look at the possibility of developing guidelines for the protection of privacy rights in relation to the use of biometrics.

Privacy Advisory Committee

The Privacy Advisory Committee (PAC) is a statutory organisation created by the *Privacy and Personal Information Protection Act 1995* NSW with members appointed by the NSW Attorney General. The members of the Privacy Advisory Committee come from a wide-ranging spectrum in the community. The Committee meets with the Privacy Commissioner and senior staff of the agency to discuss current and future projects. Members of the PAC also suggest courses that can be followed which will benefit members of the community.

Members of the Committee are able to bring a new perspective to the work of the Privacy Commissioner. All members of the office are grateful for the insights and different approaches to problems that result from meetings of the PAC. In the 2006 -07 financial year the PAC met on 18 October 2006 and 5 March 2007.

The members of the Committee were:

- Ms Alison Peters, Unions NSW
- Mr William Grant, Legal Aid Commission
- Ms Mary Elizabeth Bolt, Non-judicial member of the ADT
- Mr William James Madden, Slater and Gordon lawyer
- Honourable Penelope Gail Sharpe, MLC

Recommendations for future action arising from 2006-07 PAC Meetings

- Privacy NSW (PNSW) should consider liaising with Law Access for assistance with requests for advice and information. PNSW would need to provide training. It was also suggested that training be provided to Community Legal Centres for the same purpose. PNSW may wish to consider some form of MOU with these organisations, in order to undertake a coordinated program.
- PNSW should also consider using the LIAC system, which is a state-wide system run through the State Library. Privacy NSW might wish to consider placing links to LIAC and other appropriate research websites on its lawlink site. This should include consideration of links to Community Legal Centres as well.
- Consideration should be given to starting up the Privacy NSW newsletter again, or at least disseminating more broadly the information, which appears in the "What's New" section on the homepage of the lawlink website. It may be worthwhile to use the (updated) list of email addresses of NSW government PCOs, so that additions to "What's New" can be notified to the subscriber list via email.
- Community Legal Centres should also be added to any general mailing list.
- It may be worthwhile to start considering some variation on a privacy loose-leaf service, or perhaps Privacy NSW should consider contributing to the professional loose-leaf services, providing it with our "What's New" information, particularly in regard to any additions/deletions pertaining to directions, codes of conduct and privacy legislation, so that interested parties may be kept up to date.

Note: At least one loose-leaf service already publishes Privacy NSW's additions to "What's New".

Appendix 1– Financial Statements 2006 - 07

	Actual $	Budget $
TOTAL REVENUE	**2**	**0**
EXPENSES		
Total Employee Related Payments	723,840	643,937
Other Operating Expenses	275,044	301,443
Total Depreciation	161,061	56,095
Total Maintenance	479	455
TOTAL EXPENSES	**1,160,424**	**1,001,930**
Less: Revenue	2	0
NET COST OF SERVICES	1,160,426	1,001,930
Less: Depreciation	-161,061	-56,095
Less: Crown Liabilities	-100,176	-44,616
NET POSITION	**899,189**	**901,219**

Appendix 2 – Publications Available From Privacy NSW

Below is an abridged list of publications available from Privacy NSW. A complete list can be found on our website at www.lawlink.nsw.gov.au/privacynsw

Publication name	Format	Status	Purpose
Handbook to Health Privacy	PDF	Existing	A plain English guide to the *Health Records and Information Privacy Act 2002*
Statutory Guidelines–use or disclosure of health information for the management of health services	PDF, Word	Existing	Legally binding document that defines the scope of an exemption to the health privacy principles
Statutory Guidelines–use or disclosure of health information for training purposes	PDF, Word	Existing	Legally binding document that defines the scope of an exemption to the health privacy principles
Statutory Guidelines–use or disclosure of health information for research purposes	PDF, Word	Existing	Legally binding document that defines the scope of an exemption to the health privacy principles
Statutory Guidelines–notification when collecting health information about a person from someone else	PDF, Word	Existing	Legally binding document that defines the scope of an exemption to the health privacy principles
Privacy and people with decision-making disabilities	Hardcopy, PDF, Word	Existing	Assistance for agencies to apply the PPIP Act in a manner that protects and promotes the privacy of people with decision-making disabilities.
Privacy and Personal Information Protection Act: A Plain English Guide (1999)	Hardcopy	Existing	A plain English guide to the *Privacy and Personal Information Protection Act 1998*
A Guide to Making Privacy Codes of Practice (1999)	Hardcopy	Existing	As per title
A Guide to Making Privacy Management Plans (1999)	Hardcopy	Existing	As per title
A Guide to Internal Reviews (2000)	Hardcopy	Existing	As per title
A Guide to Public Registers (2000)	Hardcopy	Existing	As per title
A Guide to the Information Protection Principles (2000)	Hardcopy	Existing	As per title
Annual Report 2005–06	Hardcopy, PDF, Word	Existing	Overview of functions, achievements, and provides accountability to the public.
Annual Reports 2004–05. 2003–04, 2002–03, 2000–02, 1999–2000, 1998–99	Hardcopy, PDF	Existing	Overview of functions, achievements, and provides accountability to the public.
Annual Reports 2006-07	Hardcopy, PDF, Word	New	Overview of functions, achievements, and provides accountability to the public

Appendix 3 – Statistics

Note: the Quarterly Reports we provide to government are available on our website as is the method of calculation. The reports below are obtained from reports based on the information in our PRISM database.

Table 1–Source of requests for advice*

	2006-07	%	2005-06	%
Private individual	71	44%	34	28%
State government	55	34%	61	50%
Private organisation	10	6%	7	6%
Local government	9	6%	10	8%
Other	8	5%	1	1%
Other Government	7	4%	8	7%

*percentages rounded to nearest whole number

Table 2– Advice by information / practice*

	2006-07	2005-06
Health records	38	25
All records / Practices	15	21
Personal Contact details	13	12
Financial records	12	6
Surveillance/ Physical Privacy	12	21
Criminal histories / Driving records	9	5
Council / Land title records	6	6
Investigation / Law enforcement	6	9
Data security / Storage	5	5
Electoral Rolls	5	-
Court / Tribunal Activities	4	-
Customer / Membership records	4	1
Student Records	4	-
Advertising / Direct Marketing	3	-
Employment records	3	3
Identity Records	3	7
Search / Seizure	3	-
Family / Community History records	2	3
Surveys / Research	2	3
Biometric / Physical information	2	2
Tenancy Information	1	-

* Some categories were not tallied in previous years

Table 3– Requests for advice by Privacy Principle(s)*

	2006-07	2005-06
Disclosure	62	37
Collection	30	16
All Privacy Principles	29	30
Other	24	28
Access	15	12
Use	9	26
Retention / Storage	9	12
Accuracy	2	4

* The Privacy Principles are explained in more detail in the earlier section of the Annual Report.

Table 4–Nature of enquiries

	2006-07	%	2005-06	%
Phone call	986	87.2%	1308	89%
Email	143	12.6%	141	10%
Face-to-Face	2	0.2%	9	1%

Table 5–Scope of enquiries*

	2006-07	2005-06
PPIPA	401	402
Privacy Issues in General	221	-
HRIPA	212	274
Other legislation	76	274
Surveillance / Listening Devices Acts	67	129
Commonwealth Privacy Act	56	131
Other Issues / Unknown	48	248
Criminal Records	45	-
Special Projects	17	-
Public Register	6	-

* Some categories were not tallied in previous years.

Table 6–Enquiries by information/practice*

	2006–07	2005–06
Other	302	-
Personal contact details	186	111
Health records	135	279
Surveillance	132	269
Financial / Tax records	55	41
Employment records	47	63
All records / practices	47	37
Criminal records	37	119
Customer / Membership records	19	38
Investigation / Law enforcement	17	33
Photographs - taking / publishing	15	-
Biometric / physical information	14	-
Tenancy information	14	31
Council / Land title records	12	50
Data security / Storage / Archiving		24
Marketing /Spam		20
Student records		18
Identity / Age records / Identity theft		9

* Some categories were not tallied in previous years.

Table 7–Enquiries by Privacy Principle(s)*

	2006–07	2005–06
Disclosure	305	355
Other / unknown / none	234	185
Collection	172	217
Access	122	133
Surveillance / Physical privacy	83	218
Use	68	111
All Privacy Principles	32	89
Retention / storage	25	89
Accuracy	22	29

* The Privacy Principles are explained in more detail in the earlier section of the Annual Report.

Table 8–Outcome of enquiries*

	2006–07	2005–06
Provide privacy related information	702	-
Referred (to other agency)	298	115
Advice on possible course of action	111	-
Given / sent information	51	897
Invited to write in	43	65
Other	31	-
Conciliate or settle by phone	18	-
Given general advice	8	158
Task completed	8	-
Referred to Internal Review	3	-
Unable to return call / e-mail	3	-
Action complete	2	-
Converted to advice	2	-
No action	1	-
Unable to deal	1	-
Other / not recorded	-	223

* This year's recording style varies from last years, resulting in different categories. Total number of enquiries for this year and last year are 1282 and 1458, respectively.

Table 9–Types of Respondents to Complaints*

	2006–07	2005–06
State government	55	37
Private organisation	15	27
Private individual	11	9
Local government	2	6
Other governments	1	1
Other	1	-
Media	1	-

* Some categories were not tallied in previous years.

Table 10–Complaints by information / practice

	2006–07	2005–06
Health records	37	28
Personal contact details	17	14
Other	8	0
Direct marketing / Spam	4	1
Surveillance	4	12
Council / Land title records	3	1
Financial records	1	8
Criminal records	1	7
Employment records	1	4
Data Security	1	4
Client / Customer records	1	2
Student records	1	2
Identity records	1	1
Tenancy Information	1	-
Debt collection	-	1
Investigation / Law enforcement	-	4

Table 11–Complaints by Privacy Principle(s)*

	2006–07	2005–06
Disclosure	58	47
Access	7	11
Collection	5	15
Retention / Storage	5	8
Use	5	13
Physical privacy	3	5
Other	2	1
Accuracy	1	2
All Privacy Principles	1	0

* The totals in this table reflect the fact that many complaints cover more than one Privacy Principle. The Privacy Principles are explained in more detail earlier in the Annual Report.

Table 12–Outcome of complaint

	2006–07	%	2005–06	%
Matter discontinued	30	41%	19	21%
Referred to Internal Review	19	26%	2	2%
Unable to deal	9	12%	2	2%
Declined to deal	6	8%	17	18%
Conciliation / investigation	4	5.5%	27	29%
Referred to other body	4	5.5%	25	27%
Other	1	2%	0	0%

Table 13–Internal Review by Privacy Principle *

	2006–07	2005–06
Disclosure	85	79
Access	5	10
Collection	5	5
Retention / Storage	5	5
Other	3	0
Accuracy	2	4
Use	2	17
All Privacy Principles	1	5

* The conduct or decision subject to an Internal Review may cover more than one IPP or HPP. Internal Reviews must be about the IPPs or HPPs, not any other more general privacy matters.

**Table 14–Internal Reviews by information / practice * **

	2006–07	2005–06
Health records	44	20
Personal contact details	17	25
Council / land title records	9	4
Criminal records	7	9
Student records	6	8
Employment records	4	10
Court/tribunal activities	3	1
Surveillance / physical privacy	2	6
Data Security	1	5
Client / customer records	1	1
Financial records	-	5
Investigation / law enforcement	-	3
Tenancy	-	2
Identity/identity theft	-	1
Research	-	0

* The totals reflect the fact that more than one category may be selected for each Internal Review.

**Not all categories were recorded this year.

Table 15–Results of internal reviews *

	2006–07
Internal review completed	66
Complainant withdrew	4
No further contact with complainant	2
Decline to deal	1
Matter discontinued	1
No further action	1
Out of time lodgement	1
Other	1

*The categories were different last year.

Appendix 4 – Glossary Of Terms

ALRC	Australian Law Reform Commission
APEC	Asia-Pacific Economic Cooperation
APPA	Asia Pacific Privacy Administrators Forum
CCTV	Closed Circuit Television
DPP	Data Protection Principle
HPP	Health Privacy Principle
HRIP Act	*Health Records and Information Privacy Act 2002*
IPP	Information Protection Principle
MOU	Memorandum of Understanding
NPP	National Privacy Principle
OECD	Organisation for Economic Co-operation and Development
OPC	Office of the Privacy Commissioner (Cth)
PAC	Privacy Advisory Committee
PAW	Privacy Awareness Week
PCO	Privacy Contact Officer
PDF	Portable Document Format
PNSW	Privacy NSW, Office of the NSW Privacy Commissioner
PPIP Act	*Privacy and Personal Information Protection Act 1998*
PRISM	Privacy Records Information System, the database of Privacy NSW
PTP	PPIP Act Training Program
The Tribunal	Administrative Decisions Tribunal

Summary of the Complaints Process

Is Your Complaint About...

A NSW public sector agency or local council concerning your health or personal information?

> You may apply to the agency or council to have them undertake an internal review. If you are not satisfied with their findings, you may appeal to the Administrative Decisions Tribunal.

OR

> You may make a complaint directly to Privacy NSW and we may investigate and attempt to conciliate your complaint.

An Australian Commonwealth Government Department or a private sector organisation concerning your personal (but not your health) information?

> You should contact the Office of the Privacy Commissioner (Commonwealth).

The Commonwealth Office contact details:
Office of the Privacy Commissioner
GPO Box 5218
Sydney NSW 2001
or
1300 363 992

A private sector Health Service Provider or organisation and is about your health information?

> You may make a complaint to Privacy NSW and we may investigate and attempt to conciliate the matter

OR

> You may make a complaint with the Office of the Privacy Commissioner (Commonwealth).