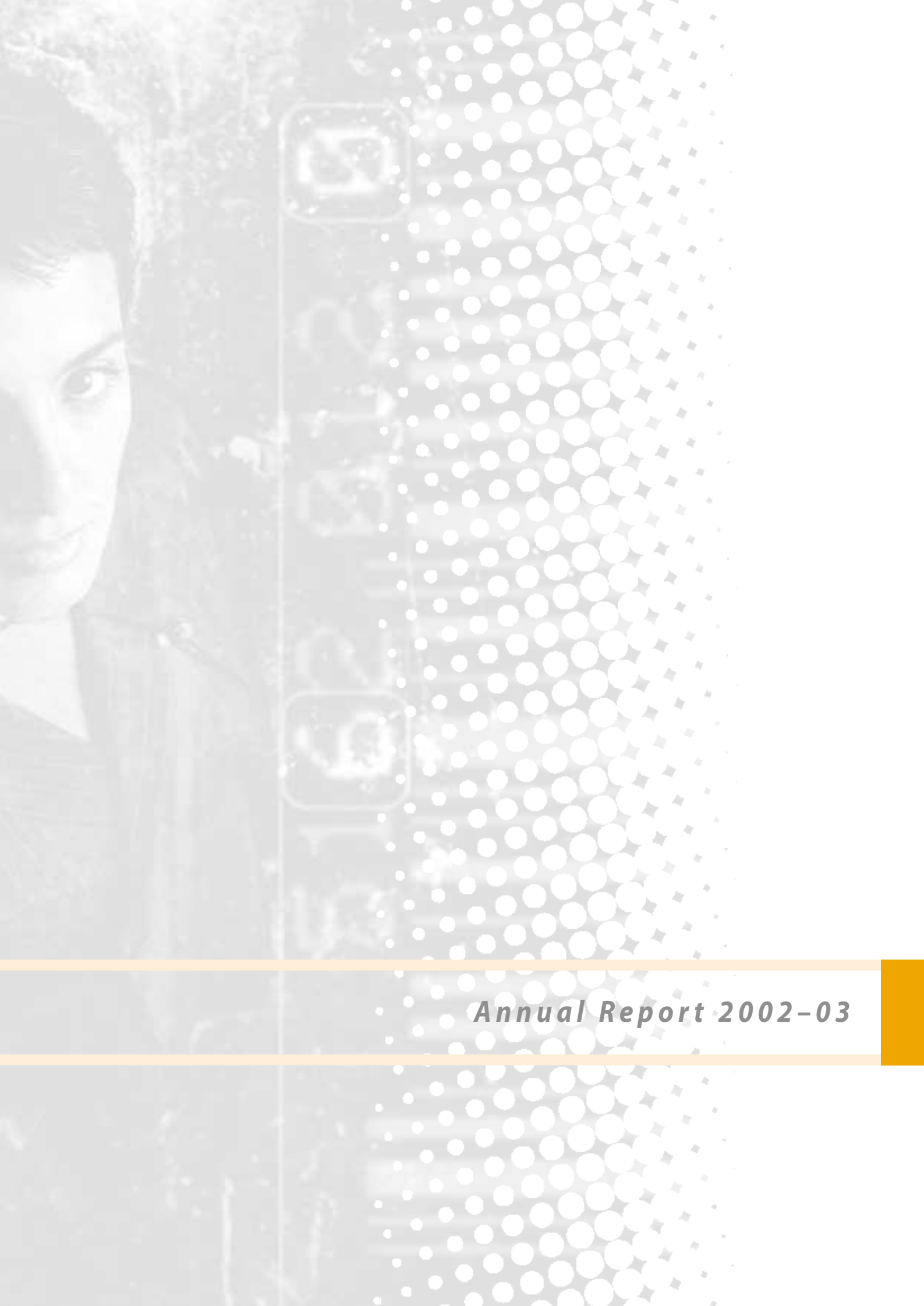


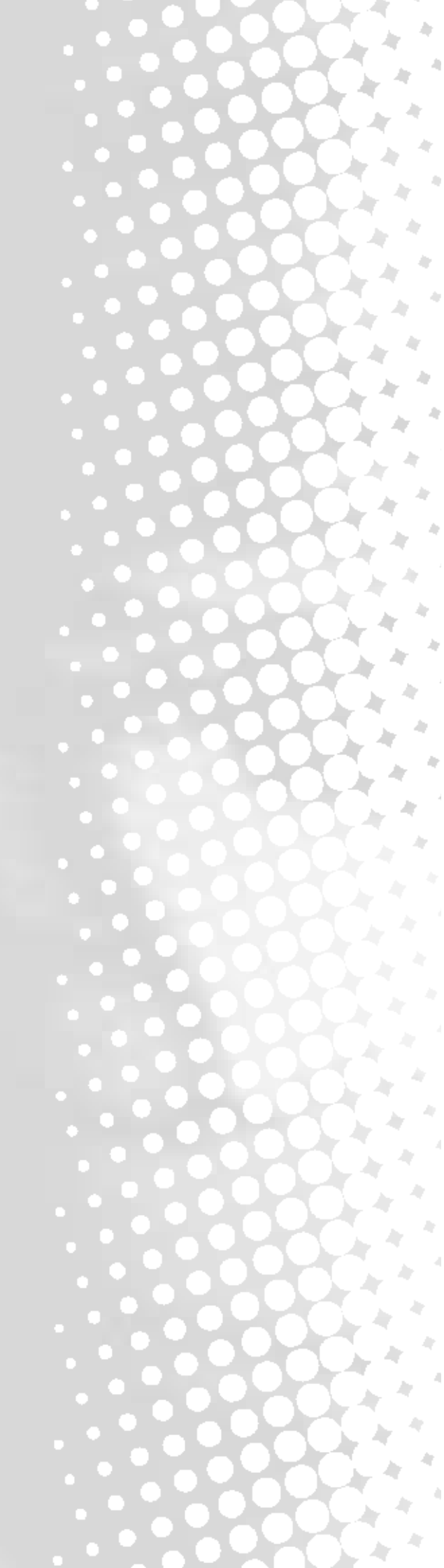


Annual Report 2002-03

privacy**nsw**



Annual Report 2002-03



The Hon Bob Debus MP
Attorney General,
Minister for the Environment
Level 36 Governor Macquarie Tower
1 Farrer Place
Sydney NSW 2000

Dear Attorney,

In compliance with section 64 of the *Privacy and Personal Information Protection Act 1998*, I have the honour to submit the Annual Report of Privacy NSW for the reporting year 2002–03.

Yours faithfully



John Dickie
Acting Privacy Commissioner

Contents

About Privacy NSW	4
How to contact Privacy NSW	4
From the Commissioner	5
Privacy in the Public Eye	6
About the PPIP Act	8
The Information Protection Principles	8
Three-Year Overview	10
The Year in Brief	11
Protection of Privacy	13
The Year in Review	13
Advice	13
Advice Case Studies	16
Enquiries	19
Complaints	21
Complaints Case Studies	24
Legislative Framework	27
The Year in Review	27
Internal Reviews	27
Outcome of Internal Reviews	28
Privacy NSW Oversight Role	29
Internal Review Case Studies	31
Applications to the Administrative Decisions Tribunal	36
Section 41 Directions	37
Education and Research	39
Training, Speeches and Presentations	39
OIT Privacy and Personal Information Protection Guideline	40
Publications	40
Consultation and Partnerships	43
Participation in Working Parties	43
Consultation on Consent and Capacity Guidelines	43
Privacy Agencies of New Zealand and Australia (PANZA+)	44
Privacy Advisory Committee	45
Privacy Roundtable	45
Administration and Staff Development	47
Organisational Restructure and Growth	47
Major IT Reform Project	48
Client Service Delivery	48
Corporate Services	49
Staff Development and Training	49
Appendix	50
Financial Statements 2002-03	50
Publications Available from Privacy NSW	50
Categories of Information or Practice at Issue	51
Glossary of Terms	52

ABOUT PRIVACY NSW

Privacy NSW is the Office of the NSW Privacy Commissioner, established on 1 February 1999 under the *Privacy and Personal Information Protection Act 1998*. 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 world's best privacy practice by all holders of personal data, particularly NSW Government agencies, thereby promoting an increased level of trust in the community, especially between people and their government.

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 into privacy complaints
- by **appearing** in the Administrative Decisions Tribunal in the review of privacy cases.

HOW TO CONTACT PRIVACY NSW

Mail: PO Box A123,
Sydney South NSW 1235

Office: Level 17, 201 Elizabeth Street,
Sydney NSW 2000

Phone: (02) 9268 5588

Fax: (02) 9268 5501

Email: privacy_nsw@agd.nsw.gov.au

www.lawlink.nsw.gov.au/privacynsw

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



FROM THE COMMISSIONER

In these early years of the new millennium, we seem to be bombarded with stories from the frontiers of science and technology - the possibilities of human cloning, even tinier hidden cameras, the rebuilding of damaged spinal cords from embryonic cells, iris-scanning machines, cars that know how to navigate streets and whether you are falling asleep. Each new development brings with it ethical dilemmas, concerns about abuse of power, and questions about accountability for the use of personal information. Where technological change brings with it the potential to diminish the privacy of individuals, we require careful examination and weighting against other public and private interests.

In 2002-03 we marked the 50th anniversary of Watson and Crick's discovery of DNA. Advances in this technology have allowed the use of DNA to identify suspects in criminal investigations to improve markedly in sophistication, and with it the use of DNA evidence to review previous convictions. During 2002-03 the Privacy Commissioner sat on both the Innocence Panel and the oversight committee for the DNA laboratories that operate DNA testing on behalf of NSW Police. More on the role of Privacy NSW in assisting government with the formulation of policy and appropriate accountability and oversight mechanisms is found on page 43 of this Annual Report.

In May 2003 the ground-breaking report *Essentially Yours: The Protection of Human Genetic Information in Australia* was released by the Australian Law Reform Commission and Australian Health Ethics Committee of the National Health and Medical Research Council. Their review covered the gamut of privacy issues arising from the use of DNA for identification / forensic, medical / research, and kinship / familial purposes. More on the review and Privacy NSW's input into the final Report is found on page 19 of this Annual Report.

But it is not only at the cutting edge of new technology that we see privacy challenges. A core tenet of privacy rights is the ability of people to control the use of their own personal information. The giving or refusing of consent is often at the heart of how we understand the ability to exercise that control - but how can this be achieved for people who have

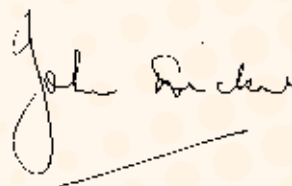
a decision-making disability? During 2002-03 Privacy NSW started to address that issue in an innovative way; see pages 40 and 43 of this Annual Report for more on that project.

The past year also saw a year of growth and change at Privacy NSW. From a significant organisational restructure early in the year, through the phase of recruitment of staff with new skills and a fresh perspective, to the commencement of a major IT and corporate services reform project towards the end of the period, Privacy NSW has sought to adapt to the changing environment, to better service the needs of its clients and stakeholders.

However in presenting this Annual Report of the work of Privacy NSW for the year 2002-03, I must immediately state that I can claim no credit for that work. Following the resignation of Chris Puplick in May 2003 after more than four years as the inaugural Privacy Commissioner of NSW, Maureen Tangney was Acting Privacy Commissioner for the remainder of 2002-03.

I was appointed Acting Privacy Commissioner from 2 September 2003, some months after the end of the reporting period. I have nonetheless been privy to the results of the dedication, hard work and commitment maintained during 2002-03 by the staff of Privacy NSW, during some challenging times. Performance standards were not only maintained but improved upon, and a number of exciting new initiatives in the areas of advice, education and training were launched. I see the reporting year of 2002-03 as a very strong foundation, upon which we will continue to build in 2003-04 and beyond.

I am therefore pleased to present to you the Annual Report for 2002-03.



John Dickie
Acting Privacy Commissioner

PRIVACY IN THE PUBLIC EYE

During 2002-03 the topic of privacy made regular appearances in the news. Here we present just the briefest selection.

\$178,000 FOR BREACH OF RIGHT TO PRIVACY

A landmark judgment in the Queensland District Court (*Grosse v Purvis* [2003] QDC 151) in June 2003 was the first Australian decision to recognise a common law tort of "invasion of privacy". Damages of \$178,000 were awarded to the plaintiff following a pattern of stalking and harassment by the defendant. The court's findings were based on comments made by judges of the High Court in the recent case of *ABC v Lenah Game Meats*, which left the way open for legal recognition of a common law right to privacy.

While the mainstream media focussed on the more sensational aspects of the particular case, privacy advocates and specialist commentators found the precedential value of the case to be of more interest.

Judge Skoien found (at para 444) that the elements of a cause of action for invasion of privacy are:

- (a) a willed act by the defendant,
- (b) which intrudes upon the privacy or seclusion of the plaintiff,
- (c) in a manner which would be considered highly offensive to a reasonable person of ordinary sensibilities,
- (d) and which causes the plaintiff detriment in the form of mental, psychological or emotional harm or distress or which prevents or hinders the plaintiff from doing an act which she is lawfully entitled to do.

Judge Skoien also noted that a defence of "public interest" should be available.



NEW TECHNOLOGIES

New technologies, the claims made about them by their investors, vendors and purchasers, and the privacy implications arising, are often in the news. For example, 2002-03 marked the first widespread sale of camera and video mobile phones in Australia, which led to countless articles about peeping toms in poolside change-rooms.

Perhaps a more disturbing product being touted during the year was a new test kit designed to help parents track their daughters' sexual activities. The kit uses a semen detection system which identifies semen on undergarments or other clothing. The product understandably horrified Australian specialists in adolescents, who noted that trust, respect and open communication are a much better way to deal with parent-teenage relationships.

And then there are the stories about the technologies that falter. A new \$90,000 iris-scanning machine, launched for testing at a Sydney gaol in March 2003, failed to recognise NSW Premier Bob Carr. The Premier joked that the cause of malfunction was that he had no criminal instincts, while a press secretary later explained that the machine was thrown by the lights of the television crews attending the launch.

BOTPA BLOOPERS

What is a BOTPA Blooper?

The phrase, coined by the former New Zealand Privacy Commissioner, means “Because Of The Privacy Act”, and refers to cases where privacy legislation is inaccurately or unfairly blamed for certain events or behaviour. For example...

Teachers and violent students

Claim: In April 2003 the *Daily Telegraph* claimed that “teachers are being denied information about violent children in their classes because of privacy laws”. The Teachers Federation lodged a dispute in the Industrial Relations Commission over the issue.

Fact: There must of course be a sensible balance between privacy and health and safety matters. The NSW privacy legislation strikes that balance through specific exemptions that recognise obligations to safeguard health and safety.

The privacy obligations on public sector agencies holding personal information do not stop the agency providing the information to appropriate persons, where the disclosure is *authorised, required or permitted* under the *Occupational Health & Safety Act*. Furthermore, the *Privacy and Personal Information Protection Act* (PPIP Act) does not prevent the disclosure of health information in circumstances where “the disclosure is necessary to prevent a serious or imminent threat to the life or health” of any person.

In response to this issue, Privacy NSW participated in an inter-agency project, headed by the Public Employment Office, to develop guidelines to better clarify where occupational health and safety obligations end, and privacy obligations start.

Accuracy of fines

Claim: In late June 2003, in a series of articles and letters to the Editor in the *Daily Telegraph*, the operations of the State Debt Recovery Office (SDRO) were criticised. The allegations included failure to check the identity of a fine recipient, failure to check whether the fines had already been paid, and failure to check that the person was still alive. It was suggested by some commentators (not the SDRO itself) that “privacy law” was the cause of these failures.

Fact: Privacy laws in NSW ensure that government departments act fairly in the way in which they collect, store, use and disclose our personal information. One of the main principles of privacy protection is ensuring the *accuracy* of information held and used by government agencies.

Privacy laws do not prevent organisations such as the SDRO from ensuring their information is accurate before they act upon it. In fact, the law aims for the opposite. Under IPP 9 (s.16 of the PPIP Act) the SDRO, like all public sector agencies, is obliged to not use personal information without first taking reasonable steps to ensure that the information is relevant, accurate, up to date, complete and not misleading.

Both the *Fines Act* and the PPIP Act allow the SDRO to collect personal information from other government sources, such as the RTA, to ensure their information is correct before fines are issued. Nor do the privacy laws prevent those other government agencies from providing their information to the SDRO, where the disclosure is lawfully *authorised, required, or permitted* under another Act.

ABOUT THE PPIP ACT

The *Privacy and Personal Information Protection Act 1998* (PPIP Act) deals with the way public sector agencies in NSW manage personal information. It was passed in 1998 in order to offer the people of NSW 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 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 the Commissioner functions that in the past were carried out by the Privacy Committee. These include the functions of conducting research, providing advice and handling complaints about breaches of privacy. The Privacy Commissioner was also given new functions (such as overseeing Internal Reviews and assisting the Administrative Decisions Tribunal in privacy cases) and additional powers (such as Royal Commission powers of investigation).

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 Information Privacy Principles in the *Privacy Act 1988* (Cth) which in turn

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 or honesty is an essential element of the financial economy.

In other instances it is necessary to 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 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.

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 public sector agencies. They are summarised here:

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 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 or 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

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.

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. You can only disclose the information for a related purpose if you believe 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, health or sexual activities or trade union membership. You can only disclose sensitive information without consent in order to deal with a serious and imminent threat to any person's health or safety.

THREE-YEAR OVERVIEW

This section provides a brief look at the evolution in our workload since the commencement of the *Privacy and Personal Information Protection Act* on 1 July 2000:

- A 27% increase in the number of requests for advice (Figure A)
- A 63% increase in the number of telephone, email and face-to-face enquiries (Figure B)
- A 15% increase in the number of formal complaints lodged (Figure C)
- Almost a four-fold increase in new Internal Review applications (Figure D)
- More than a ten-fold increase in matters lodged in the Administrative Decisions Tribunal (Figure E).

Figure A – New advice workload, 2000-01 and 2002-03

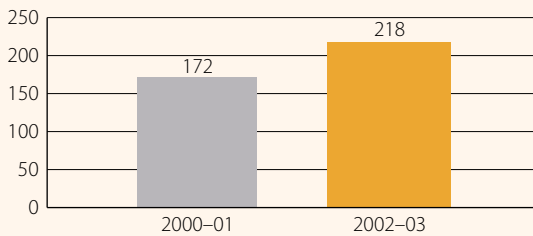


Figure B – New informal enquiries workload, 2000-01 and 2002-03

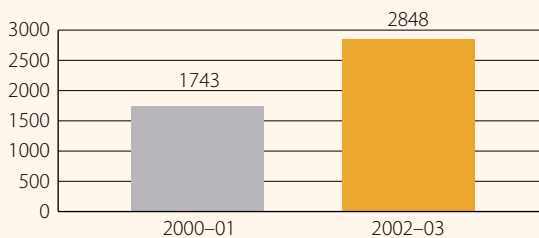


Figure C – New complaints workload, 2000-01 and 2002-03

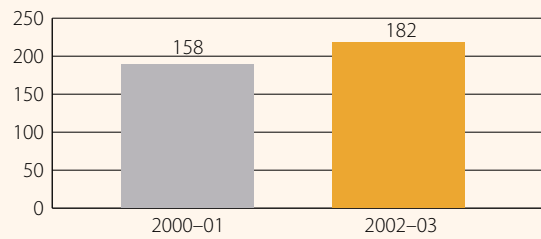


Figure D – New Internal Review workload, 2000-01 and 2002-03

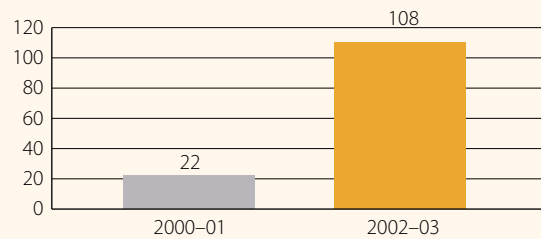
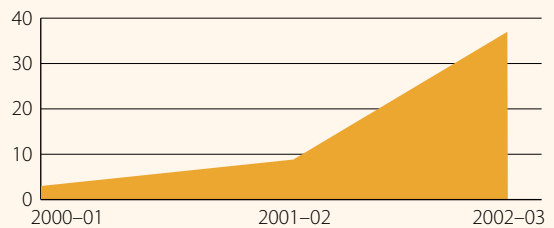


Figure E – Number of ADT cases lodged per year, 2000-01 to 2002-03



THE YEAR IN BRIEF

Our achievements for each key result area in the reporting period include:

Key Result Area	Achievements
<p>PROTECTION OF PRIVACY</p> <p>To protect and promote the privacy of individuals by providing advice and handling complaints.</p>	<ul style="list-style-type: none"> ▶ finalising 2,848 enquiries, 230 formal advices and 221 complaints ▶ improving by 16% the timeliness of dealing with complaints ▶ finalising 83% of formal requests for advice within 12 months ▶ publishing <i>Child Offenders and Privacy</i>.
<p>LEGISLATIVE FRAMEWORK</p> <p>To ensure the robust nature of privacy laws in New South Wales.</p>	<ul style="list-style-type: none"> ▶ completing 72 Internal Review matters ▶ assisting the Administrative Decisions Tribunal at planning meetings for 34 new matters, and at hearings for 10 privacy review cases ▶ making two new section 41 Directions ▶ launching the Internal Review checklist and application form ▶ preparing for the commencement of the <i>Health Records and Information Privacy Act 2002</i>.
<p>EDUCATION & RESEARCH</p> <p>To empower people to exercise greater control over their personal data, and to encourage NSW public sector agencies to respect the privacy of their clients.</p>	<ul style="list-style-type: none"> ▶ presenting 21 speeches and training sessions ▶ launching the OIT <i>Privacy and Personal Information Protection Guideline</i> ▶ hosting the Law Week forum on 'consent and capacity' issues ▶ launching the <i>Draft Guidelines on Consent and Capacity</i> for public consultation.
<p>CONSULTATION & PARTNERSHIPS</p> <p>To build mutually beneficial partnerships with clients, stakeholders and other privacy agencies.</p>	<ul style="list-style-type: none"> ▶ hosting the PANZA+ meeting, November 2002 ▶ participating in eight inter-agency working parties ▶ giving evidence at two Parliamentary Inquiries ▶ holding a public consultation on the <i>Draft Guidelines on Consent and Capacity</i>.
<p>ADMINISTRATION & STAFF DEVELOPMENT</p> <p>To ensure that the administrative framework of Privacy NSW supports all officers in their work, and that the skills and talents of staff are utilised in the workplace.</p>	<ul style="list-style-type: none"> ▶ implementing an organisational restructure ▶ commencing the IT reform project ▶ signing a Memorandum of Agreement with NSW Health ▶ developing specific in-house training on client service skills.



To protect and promote the privacy of individuals through providing advice and handling complaints

Protection of Privacy

THE YEAR IN REVIEW

A number of functions and activities fall under the broad heading of 'the protection of privacy'. The activities reported in this section are:

- The provision of formal written advice
- The provision of informal advice, assistance or referral for telephone, email and face-to-face enquiries
- The investigation and conciliation of complaints.

Our timeliness in dealing with these functions improved again in 2002-03, most notably with a 16% improvement in the time taken to finalise complaint matters. The number of enquiries we received continued at the same high levels reached last year, with the majority resolved within 24 hours. Mostly these are telephone enquiries, handled by staff across the organisation rather than by dedicated enquiries staff.

In addition to advising public sector agencies on how to comply with existing legislation, our advice function also includes commenting on proposed new laws. For example in July 2002 we published a position paper on *Child Offenders and Privacy*, following public debate about the naming of child offenders involved in a series of gang rapes in Sydney. Our advice function also includes commenting on reviews of existing laws in terms of their privacy impacts. During 2002-03 for example we made submissions to the office of the NSW Ombudsman with respect to his review of the *Police Powers (Internally Concealed Drugs) Act 2001*.

The passage of the *Health Records and Information Privacy Act* (HRIP Act) in the latter half of 2002 also signalled a shift in both our complaints handling and advice provision for the future, as the private sector will be regulated when the Act commences in 2004. Preparation for commencement of the HRIP Act began during 2002-03.

This new legislation coincided with a significant increase in the importance of health records, in terms of the numbers of both informal enquiries and formal complaints dealt with during 2002-03, compared to previous years.

Also in relation to complaints, we noticed a trend in which complaints about private sector organisations are increasingly being made by their own employees. This may be because there is an exemption for 'employment records' in the private sector coverage of the Federal *Privacy Act 1988*. Employees of private sector organisations therefore do not have enforceable privacy rights under the Federal scheme, but may approach Privacy NSW to seek conciliation of their complaint.

Another noticeable trend was that requests for advice on biometric and related physical information increased significantly this year, as did requests relating to investigation and law enforcement practices.

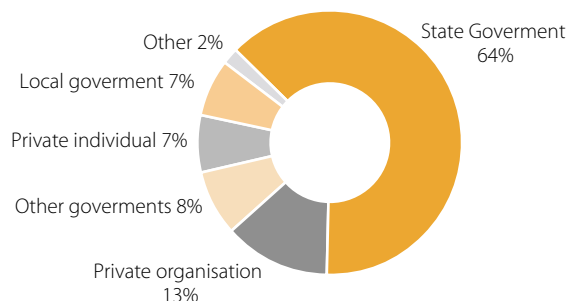
ADVICE

The advice that we provide includes applications for formal advice, investigations launched on the Privacy Commissioner's own initiative and requests to make presentations and hold training sessions.

In 2002-03, we opened 218 new advice files, and closed 230. Almost 83% of advice files were closed within 12 months of being opened. This represents a 33% improvement in the timeliness of files being dealt with, compared to two years previously. The following analysis relates to the 230 files finalised during 2002-03.

Nearly two-thirds of requests for advice came from State Government agencies, followed by private organisations (Figure 1). The percentage of requests for advice from

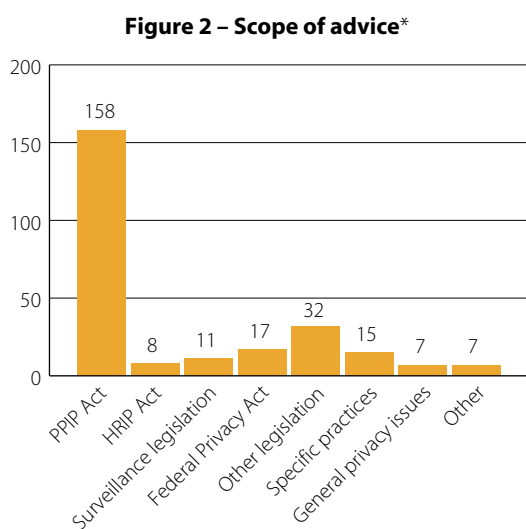
Figure 1 – Source of requests for advice



private organisations, which had accounted for one-fifth of requests in the previous year, decreased this year, as many private sector privacy issues are now being covered by the Office of the Federal Privacy Commissioner under the Federal *Privacy Act 1988*.

The great majority of advice requests related to the application of the PPIP Act, although the new HRIP Act also appeared in our figures for the first time (Figure 2). Various types of surveillance legislation (listening devices, workplace video surveillance, etc) were covered in 11 requests for advice, and 32 included advice on other legislation, whether existing legislation or legislative proposals such as draft Bills. Fifteen advices given included commentary on specific projects and/or practices, and 17 incorporated advice about the Federal *Privacy Act*. These figures are consistent with the previous year.

Requests for advice cover a wide spectrum of subjects or practices. Major topics covered were health records, surveillance and physical privacy, investigation and law enforcement practices, council and land title records

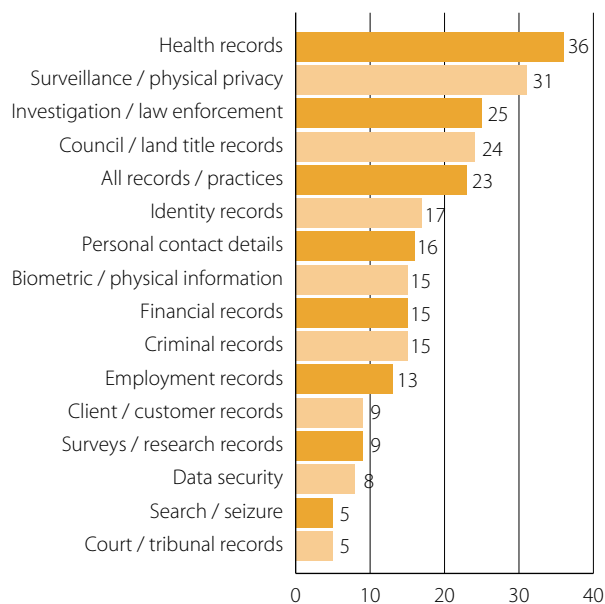


* The scope of a request for advice can cover a number of subjects, which is why there are more than 230 responses in this figure.

and identity records (Figure 3). Requests for advice on biometric and related physical information (such as DNA issues), and investigation and law enforcement practices, increased noticeably since the previous year. By contrast requests for advice with respect to personal contact details dropped since 2001-02.

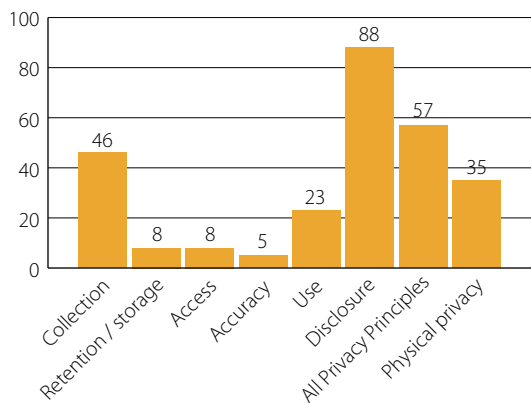
As in previous years, both disclosure and collection stand out as the two most common areas relating to informational privacy on which advice was sought, with 38% and 20% of advices incorporating those areas respectively (Figure 4). Compared to previous years there has been a growth in the relative importance of the use of personal information and physical privacy issues.

Figure 3 – Advice by information / practice*



* The top 16 categories only are presented in this figure. The totals reflect the fact that more than one category may be selected for each advice. For the full list of all subject categories see Appendix 3.

Figure 4 – Advice by Privacy Principle(s)*



* The totals in this graph reflect the fact that many advice matters cover more than one Privacy Principle. Where more than three Privacy Principles were identified, the advice was classified instead under "All Privacy Principles". The Privacy Principles are explained in more detail in the box on this page, *What do we mean by a Privacy Principle?*



WHAT DO WE MEAN BY A PRIVACY PRINCIPLE?

In the PPIP Act there are 12 *Information Protection Principles*; in the HRIP Act there are 15 *Health Privacy Principles*. When we deal with other privacy issues not regulated by the PPIP Act or the HRIP Act, we might use the *Data Protection Principles*. So when describing our work, should we talk about IPPs, HPPs or DPPs?

Each of these sets of Privacy Principles has a generic basis in the 'information life cycle'. The 'information life cycle' is a way of describing the manner in which personal information is dealt with by an organisation, starting with the collection, then the storage of the information, access by individuals, use, disclosure and eventual disposal by the organisation. The concept of the 'information processing cycle' or 'information life cycle' has been part of Australian privacy regulation since the 1983 Australian Law Reform Commission Report on Privacy.

By contrast physical privacy issues are usually analysed with reference to the Prosser tests (see *What is privacy?* on page 8).

The Privacy Principles described here are therefore an attempt to use generic categories, so as to enable comparison across different legislation or jurisdictions. They incorporate both physical privacy and informational privacy.

ADVICE CASE STUDIES

THE DISPOSAL OF HUMAN TISSUE

Following a recommendation by the Australian Health Ethics Committee on the ethical disposal of human tissue and organs collected at autopsy, we were asked to advise NSW Health on their procedures for consulting with families about disposal. The Department proposed providing information about the deceased to immediate family members to ascertain their views about how retained material should be disposed of. This could include health information to assist their decision-making.

The collection of information by NSW Health from other agencies and the disclosure of health information about a person to family members would normally require the person's consent. In the case of information about a deceased person, obviously the person is unable to give their consent. Information about recently deceased people is included in the PPIP Act's definition of personal information, as is body tissue itself.

While supporting the aims of the project we considered that the current law, including NSW Health's Privacy Code of Practice, would not have permitted the proposed disclosure. We advised that the Privacy Commissioner was prepared to make a direction to expedite the family consultation process. We also discussed the need for an approach that would minimise the likelihood of further distress to bereaved family members. We also advised that cultural and other sensitivities needed to be taken into account. The Privacy Commissioner made a section 41 Direction on 24 February 2003 to support the new procedures. The Direction is currently in force until 1 April 2004.

COURTS IN THE SPOTLIGHT

There are often tensions surrounding the protection of individuals' privacy and the media's pursuit of informative and interesting material. However privacy and journalism are not incompatible. Both the protection of privacy and a free press are essential to upholding democratic values and rights such as freedom of speech.

In 2002-03, Privacy NSW provided advice to the Attorney General's Department on two proposals to film "reality TV" documentaries inside NSW courts. Documentary films can demystify how our courts and tribunals operate. However filming must be done in an accountable manner that protects the privacy and dignity of all concerned.

Filming inside sensitive environments such as courts raises even more privacy concerns than other documentaries. This is because witnesses are forced by law to tell the truth and may need to reveal damaging or embarrassing information about themselves. The public broadcast of this information may have serious consequences for a person's relationships with family, friends, employer, acquaintances and others.

Privacy NSW advised the Attorney General's Department that filming inside courts should only proceed with the informed consent of all individuals who might be affected by the broadcast. Our advice stressed that relevant professional organisations - like the police and lawyers who appear regularly in court - must be consulted about their role in filming. However of more concern was the need to ensure adequate privacy protection for the accused, witnesses, jurors, victims, and their relatives and friends in court. These individuals may be vulnerable, are the least likely to have professional representation, and may have the most to lose if they are improperly filmed in court.

The Attorney General's Department did not approve one proposal, to film inside local courts, as the production company would not agree to the recommended levels of privacy protection. However a proposal to film inside the Coroner's Court, which incorporated more rigorous privacy protections for the most vulnerable individuals, was accepted. The results were shown on ABC TV as *A Case for the Coroner*.

GUTHRIE CARDS

As a result of a *voir dire* hearing in the Supreme Court in April 2001 on the admissibility of DNA evidence, we were made aware that DNA from a Guthrie card collected for NSW Health's Newborn Screening Program had been used to identify a missing person who was presumed deceased. As this coincided with the Australian Law Reform Commission's inquiry into the protection of genetic information (see below), we made inquiries with NSW Health as to how routine such investigations were. Later in 2001 we were invited to comment on a Protocol to allow NSW Police to access Guthrie cards for limited purposes.

Blood samples from newborns have been collected and stored on Guthrie cards in NSW for more than 25 years. They are used to screen newborn children for genetic defects and to support research into genetic conditions. NSW Health has assured parents that the cards will be stored confidentially and securely. We were concerned to establish that the introduction of very broad exemptions in the PPIP Act for disclosure of information for law enforcement should not lessen this high level of security and confidentiality. We were also concerned that their availability should not provide a way around the legal safeguards for collection of DNA samples under the *Crimes (Forensic Procedures) Act*.

The Protocol recognises that Police may need access to Guthrie cards, and lays down procedures for seeking access. It emphasises that in most circumstances this access should be limited to identification of bodies and identifying crime scene remains where a victim is missing or presumed to be dead. In both instances consent should be sought from next of kin.

After the Protocol was finalised in July 2002 we became aware of some public concern that the Protocol was designed to extend Police access to the Guthrie card collection, rather than its intended objective of establishing accountable collection for a limited range of purposes. Consequently we suggested that it would be desirable to make the Protocol public. In December 2002 NSW Health advised us that a copy of the protocol had been placed on their website. We then linked to the Protocol and publicised its availability from the Privacy NSW website.

PRIVACY FOR CHILDREN

We sometimes assume that because children rely on their parents for basic decision-making, including the information needed to make decisions, that privacy does not apply to children. Sometimes this leads public sector agencies and other organisations to assume that they are free to use personal information about children without reference to them and without their consent. Children are not excluded from the requirements of the PPIP Act. Section 9 allows parents or guardians to consent to the collection of children's information from third parties and there are a number of additional exemptions in Codes and Directions made under the PPIP Act. It is important to recognise that children are entitled to the same basic privacy rights as adults, except in circumstances where such rights need to be modified to reflect their developing capacity.

A number of advice matters during the year throw light on the issue of children's privacy.

We were asked for advice when a public sector agency sought an exemption from the Act to allow it to use photographs of child clients in publicity material without seeking consent. We took the view that such an exemption was unjustified. We also advised another agency on similar issues relating to the use of photographs of child visitors. And a third incident, which became the subject of an Internal Review, highlighted children's privacy when a photograph of a child victim of a dog attack was supplied by the local council to the media, without consent from either the child or their parents. As a result of these issues we had discussions with the Commission for Children and Young People and agreed to work with them on guidelines for children's privacy. This has become a project for the next year.

The use of information about school children raises significant privacy issues. Our advice was sought on a proposal for details of all school and TAFE students to be provided to the Department of Transport, to monitor users of bus and train passes under the School Student Transport Scheme. We pointed out that such a request ought to comply with a range of obligations under the PPIP Act affecting both the Department of Education and Training as the agency holding the information, and the Department of Transport as the agency collecting it. We were also asked for advice on the overlapping responsibilities of public schools under the PPIP Act and of private sector transport operators subject to the Federal *Privacy Act*.

A similar issue involved the development of a protocol between the Department of Education and Training and NSW Police for sharing information about students as a means of reducing or minimising crime risks in schools. Our advice pointed out that under the law enforcement exemption in section 23 of the PPIP Act the Department could disclose

information which had a direct relationship to possible offences. Sharing information about risks relied on provisions of the Department's Privacy Code of Practice which permit the collection and disclosure of personal information where considered necessary to "promote a safe and disciplined learning environment". We warned that these exemptions should not be interpreted so broadly as to effectively deny students any privacy rights. We suggested that the protocol should provide the opportunity for a more detailed description of how the exemptions should be applied.

Another issue we were asked to comment on involved the development of a protocol to resolve problems about the behaviour of young people in shopping centres. This would involve collecting photographs of young people who had come to the attention of security staff. We pointed out the need for a protocol to recognise existing laws and procedures affecting retailers, including the Federal *Privacy Act*. Further development of the protocol needed to balance the interests of children and young people with those of retailers and centre management, including their right to enter and move around shopping centres without being forced to provide identification.

On a somewhat different note, in July 2002 the Acting Privacy Commissioner released a position paper on *Child Offenders and Privacy*. This was in response to heated public discussion about identifying juvenile offenders in high profile sexual offence trials. The paper supported current arrangements under the *Children (Criminal Proceedings) Act* which require the sentencing judge to balance the principles of open justice against prejudice to the child offender when determining whether to disclose the identity of people convicted of serious indictable offences committed when they were children. The paper opposed attempts to remove this protection.

THE GENE GENIE

Following on from their *Issues Paper* in March 2002 (see our 2001-02 Annual Report), the Australian Law Reform Commission and the Australian Health Ethics Committee of the National Health and Medical Research Council released a *Discussion Paper* in August 2002 on the protection of human genetic information.

In December 2002 Privacy NSW made an extensive submission on the *Discussion Paper*. A copy of our submission can be downloaded from our website.

The final report, 1200 pages long and containing 144 recommendations, was released in May 2003. The report, *Essentially Yours: The Protection of Human Genetic Information in Australia*, is the product of two years of inquiry, research and widespread public consultation. It has been well received by stakeholders such as family lawyers, geneticists, life insurance companies, as well as in the wider community.

Essentially Yours aims to strike a balance between scientific progress and the protection of privacy. Our views and advice were taken into account by the ALRC / AHEC, especially in sections dealing with 'Information and Health Privacy Law', and 'Privacy of Genetic Samples'.

The report recommends that:

- DNA parentage testing should be conducted only with the consent of both parents, or with a court order
- Employers should not be permitted to collect or use genetic information - except in rare circumstances
- Privacy laws should be harmonised and tailored to address the particular challenges of human genetic information
- A standing Human Genetics Commission of Australia should be established to provide high-level, technical and strategic advice.

ENQUIRIES

Our investigation and legal and policy officers answer phone and email enquiries from members of the public and from organisations. There is no single designated telephone enquiry officer. As in the past, the large majority of enquiries were received by telephone. We recorded over 2600 telephone enquiries, which is almost the same number as the previous year. We also received 160 email enquiries and 45 face-to-face enquiries. The total figure was 2,848 (Figure 5).

For the first time we recorded the scope of the enquiries received. Almost one-third of all enquiries received were about the PPIP Act and another third about the Federal *Privacy Act*. Other enquiries were spread across a variety of different legislation and general and specific privacy matters (Figure 6).

Figure 5 – Nature of enquiries

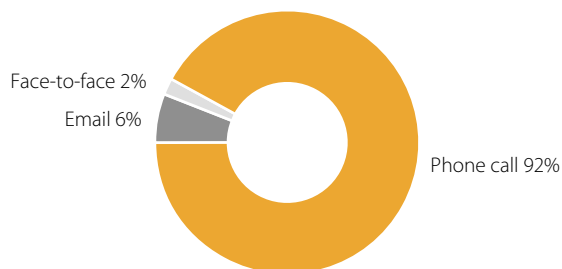


Figure 6 – Scope of enquiries

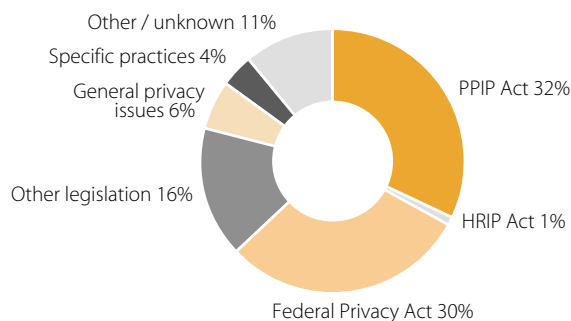
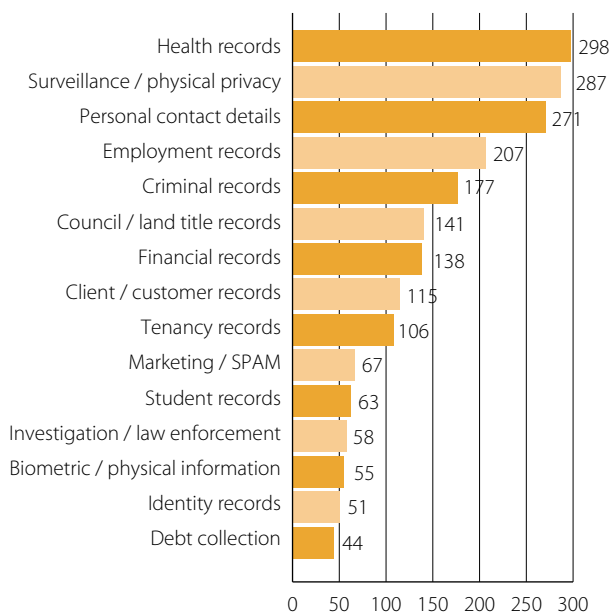


Figure 7 – Enquiry by information / practice*



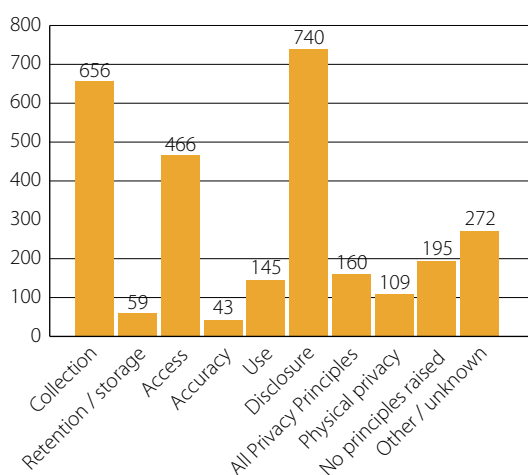
* The top 15 categories only are presented in this figure. For the full list of all subject categories see Appendix 3.

The most common type of information or practice raised in enquiries was health records, followed by surveillance / physical privacy, personal contact details and employment records (Figure 7). This marks a considerable growth in importance of both health records and surveillance, which had not featured as prominently in previous years.

This year for the first time we recorded the nature of enquiries by Privacy Principle (as we do for all advice, complaints, and Internal Review matters). Like those other areas of our work, the disclosure and collection of personal information feature the most strongly as the subject of informal enquiries. However, the enquiries also measured strong interest in the question of access to personal information (Figure 8).

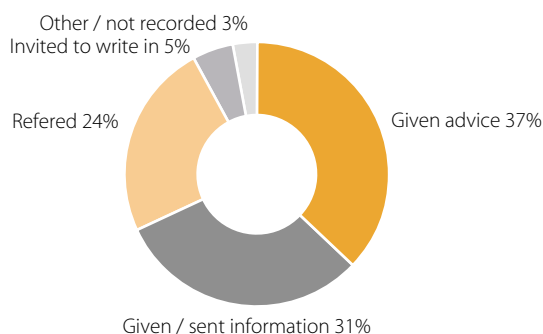
Over two-thirds of all enquiries were provided with advice or information, and 24% were referred to other organisations (Figure 9). The majority of these were referred to the Office of the Federal Privacy Commissioner (66%). This reflects the high number of enquiries we receive which actually fall under the jurisdiction of the Federal *Privacy Act 1988*.

Figure 8 – Enquiry by Privacy Principle(s)*



* The Privacy Principles are explained in more detail on page 15, *What do we mean by a Privacy Principle?*

Figure 9 – Outcome of enquiries



COMPLAINTS

Under Part 4 of the PPIP Act, Privacy NSW is responsible for accepting and considering complaints made by individuals who believe their privacy may have been violated or interfered with. Complaints range from neighbourhood disputes, to actions by private sector organisations and State Government agencies. Generally we will not investigate a complaint unless it has been lodged in writing.

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 could be resolved by referral to a more appropriate agency.

Where we decide to investigate a complaint, we must endeavour to resolve the complaint by conciliation. We seldom undertake a face-to-face conciliation process, but use correspondence to ensure that all parties to a complaint are aware of the issues and each others' views, and that the party complained about takes such steps as are considered reasonable to protect privacy in the future.

This year, we received just over 180 new privacy complaints and finalised 221, which is a slight decrease from the previous year. There was a 16% improvement in the timeliness of complaints files closed this year, with 87% of complaints finalised within 12 months.

Half of the complaints finalised in this reporting period concerned public sector agencies (either State or local government agencies) and 45% concerned private organisations. These figures are consistent with the previous year, though mark a slight increase in the complaints against the public sector (Figure 10a).

Of the 110 complaints finalised against NSW public sector agencies, agencies in the human services area feature prominently, followed by the justice sector and then local government (Figure 10b).

Figure 10a – Complaints against

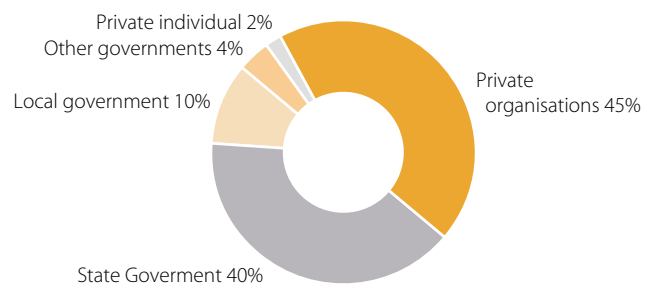


Figure 10b – Complaints against public sector agencies by sector

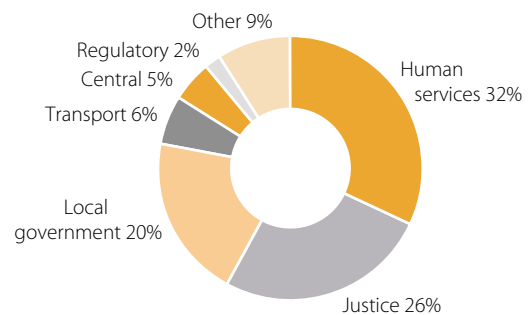
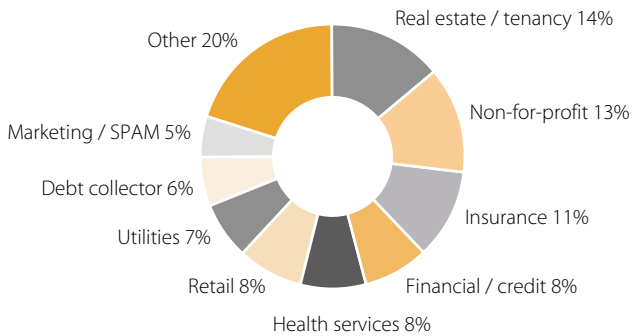


Figure 10c – Complaints against private organisations

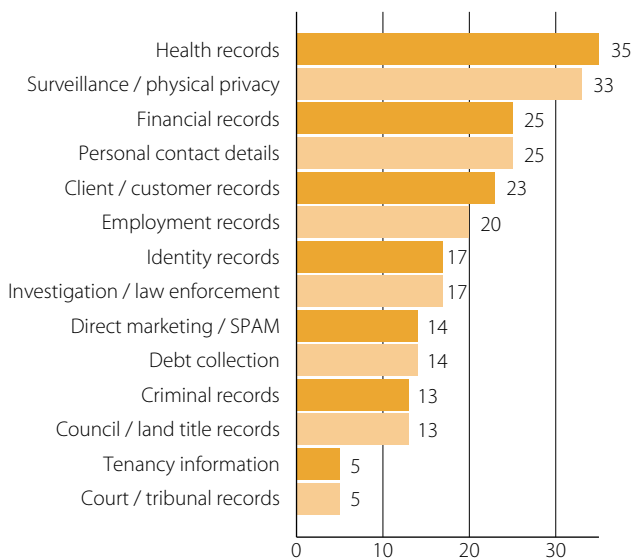


Of the 99 complaints against private organisations, it was the real estate / tenancy sector which featured the most prominently, followed closely by not-for-profit organisations, insurance companies and financial / credit institutions (Figure 10c).

Of the complaints made against NSW public sector agencies, 28 (25%) were made by clients / customers of the agency, followed by employees of the agency (18%) and residents / ratepayers (15%).

Of the complaints finalised against the private sector, just under half (47%) were made by clients / customers of the organisation concerned, and almost one-quarter (24%) were made by people who had been the subject of the respondent's unsolicited attention. Sixteen per cent were employees of the organisation, which represents a rise compared to the previous year.

Figure 11 – Complaints by information / practice*



As with the previous reporting year, the nature of information or practice at issue was spread across a wide range of matters (Figure 11). The most common categories were health records, surveillance / physical privacy, financial records and personal contact details. This represents a significant rise in the importance of health records compared to the previous year.

Of the complaints made against the public sector, the most common categories of information or practice at issue were health records, surveillance / physical privacy, identity records, and investigation / law enforcement practices.

Of the complaints made against private organisations, the most common categories were surveillance / physical privacy, financial records, personal contact details and client / customer records.

Half of all complaints finalised in this period included an alleged disclosure of personal information to third parties,

* The top 14 categories only are presented in this figure. The totals reflect the fact that more than one category may be selected for each complaint. For the full list of all subject categories see Appendix 3.

and a quarter included the collection of personal information as part of the complaint (Figure 12).

Of the 221 complaints finalised this year (Figure 13), 40% were referred to another complaints body. This figure continues to rise in relation to previous years, and is explained by the fact that we continue to receive many complaints that now come under the Federal *Privacy Act 1988*, and are therefore best referred to the Office of the Federal Privacy Commissioner.

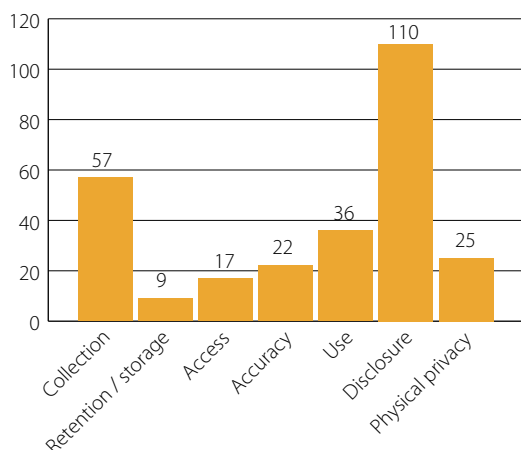
This year also saw a dramatic increase in the number of complaints referred to Internal Review; in 2002-03 this was the outcome for 24% of all complaints, compared to less than 10% the previous year. This is because the time limitations set for the introduction of Internal Review – that the conduct must have occurred since 1 July 2000 – now have less of an impact on new complaints.

These two phenomena account for the drop in the proportion of cases which proceeded to conciliation and / or investigation: 18% in 2002-03, compared to 31% the previous year.

Of the 40 matters which proceeded to conciliation and / or investigation, in five cases (12%) a "violation or interference with privacy" was found, and a report issued to the parties. A further 20 matters (50%) were resolved by conciliation without a formal finding, while four cases (10%) could not be resolved.

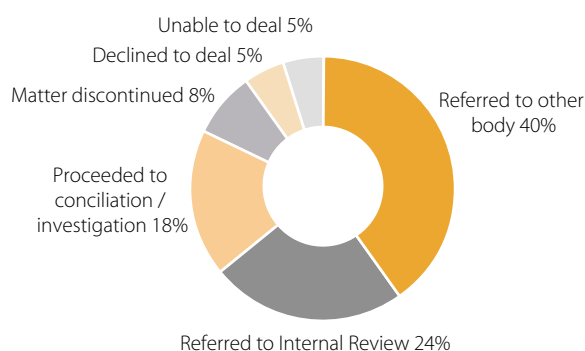
In 11 cases (28%) a finding was made of "no violation or interference with privacy". This was because the alleged conduct or decision could not be proven to have occurred (6 cases), the conduct complied with the relevant privacy standards (4 cases), or the non-compliance was authorised by an exemption (1 case).

Figure 12 – Complaints by Privacy Principle(s)*



* The totals in this figure reflect the fact that many complaints cover more than one Privacy Principle. The Privacy Principles are explained in more detail on page 15, *What do we mean by a Privacy Principle?*

Figure 13 – Outcome of complaint



COMPLAINTS CASE STUDIES

The case studies below illustrate the types of complaints we received and the way our Office seeks to resolve such matters.

CRIMINAL IDENTITY

Privacy NSW received a complaint relating to the accuracy of criminal records held by the NSW Police Service. The complaint highlighted the privacy impacts of identity theft and identity fraud, and the consequences that can arise when an individual assumes another person's identity.

The complainant (Mr A) notified us that he discovered that another individual (Mr B) had been using Mr A's name. Mr B had been arrested and charged by NSW Police on several occasions with various offences and had given his name to the Police as Mr A. Mr B had also been imprisoned. As a result, Mr A received communications from other government agencies which incorrectly stated that he had been charged with a number of offences and had recently been in prison.

Mr A complained to the NSW Police Service. He was informed that because Mr B had given a false name when he was first charged, the Police Service criminal record system would always default to the name given on the first charge. In this case Mr A's name would head the criminal record for Mr B, even though the Police subsequently discovered Mr B's real name. This effectively meant that Mr B's criminal record was recorded under Mr A's name but with a notation that his real name, Mr B, was an "alias," and included a warning that he should be charged under his real name Mr B.

Mr A complained to Privacy NSW that the Police Service was in breach of IPPs 8 and 9 (sections 15 and 16 of the PPIP Act), which provide that a public sector agency must allow you to update, correct or amend your personal information, and must make sure that your personal information is relevant, accurate, up to date and not misleading before using it.

Although section 27 of the PPIP Act provides broad exemptions for the NSW Police and other law enforcement agencies from complying with the IPPs except in relation to their educative and administrative functions, Privacy NSW contacted NSW Police on Mr A's behalf to investigate the matter.

Privacy NSW was concerned that, as a result of NSW Police's policies and procedures, the privacy impacts experienced by Mr A could always occur where an individual provided a false name to the police when first arrested, notwithstanding that the police later discovered the true identity of the individual. As a result an innocent member of the public could find that their name would remain on Police records and databases, implying that they had a criminal record, and that they went by an alias. Individuals could possibly find themselves under scrutiny for crimes which they have not committed, or if a dispute ever arose as to their identity. Furthermore, incorrect details of arrests, criminal record or other related information could also be reproduced to other organisations.

As a result of Mr A's complaint, the NSW Police agreed to take steps to establish a computerised system that would allow for a change in the "record name" of a criminal history in order to correct NSW Police records. This action would ensure that Mr B's criminal history would be recorded under his own name, and not that of the complainant Mr A. NSW Police also agreed to establish a protocol to provide future guidance as to when a criminal record may be changed.

MANAGING PROPERTY PRIVATELY

A complaint was made by an individual (Mr B) against a real estate agent. The real estate agent had been the managing agent of a property which the complainant had recently leased. At the end of the lease there were some outstanding issues between the parties, so Mr B requested that further contact be made by either his mobile telephone or new address, which he provided to the agent.

Contrary to Mr B's instructions, the real estate agent proceeded to contact Mr B at his place of work. On one occasion a letter was left at the reception desk. On another occasion a fax was sent, not marked private or confidential. Mr B was concerned that his private information was exposed to his colleagues during the working day.

Since December 2001 the Federal *Privacy Act 1988* has regulated many private businesses, such as real estate agents. However, there is an exemption for businesses which have a turnover of less than \$3 million per year. In this case Mr B was advised by the Office of the Federal Privacy Commissioner that his complaint was outside the Federal Act's jurisdiction. On this basis Privacy NSW accepted the complaint under Part 4 of the PPIP Act.

Privacy NSW asked the real estate agent to explain why it had sent correspondence to Mr B's place of work. The real estate agent responded that it contacted Mr B at work because it had no other way to contact him. The agent also advised that it had apologised to Mr B and that the matter had been amicably resolved. Mr B did not take the complaint any further.

PRIVACY FOR SALE

Mr C had changed his name by dropping his first name. He later received a letter from a real estate agent, addressed to his previous name. He was told by the agent that the information had come from RP Data and so he wrote to RP Data asking that the information be corrected. Mr C did not receive a response. Mr C's complaint did not come under the jurisdiction of the Federal *Privacy Act 1988* as the conduct occurred before December 2001.

Privacy NSW wrote to RP Data requesting that they review their records and correct their holdings to reflect Mr C's chosen name. Privacy NSW also raised concerns with the Valuer General (now part of the Department of Lands) about the manner in which RP Data use personal

NEW COMPLAINTS REFERRAL ARRANGEMENTS

During this year, Privacy NSW entered into an Information Sharing Arrangement and a 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 powers to deal with it. They therefore allow us to pass 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: http://www.lawlink.nsw.gov.au/pc.nsf/pages/omb_arrange.

information provided by the Valuer General under the *Valuation of Lands Act 1916*.

The Valuer General sells information to RP Data (and other organisations) in its capacity as a valuation body. A common method by which the Valuer General collects personal information is through the Notice of Sale provided to the Valuer General following the sale of a property. The Valuer General is authorised to disclose this information to valuers under the *Valuation of Land Act 1916*. The PPIP Regulation 2000 exempts the Valuer General from compliance with Part 6 of the PPIP Act with respect to "any valuation roll kept under the *Valuation of Land Act 1916*".

RP Data advised that the details about Mr C had in fact been removed from the listing that they sell to real estate agents. The Valuer General agreed to tighten the terms and conditions under which personal information is sold to land valuers.



To ensure the robust nature of
privacy laws in New South Wales

Legislative Framework

THE YEAR IN REVIEW

The activities reported in this section are:

- The oversight of Internal Reviews being conducted by public sector agencies into privacy complaints
- Assisting the Administrative Decisions Tribunal in reviewing conduct following an Internal Review
- Assisting the Attorney General in the development of Privacy Codes of Practice under the PPIP Act
- Making public interest determinations (“section 41 Directions”) to allow exemptions from the PPIP Act in certain circumstances
- Developing statutory guidelines under the HRIP Act.

2002-03 has been a year of consolidation for Privacy NSW, as public sector agencies settled into the rhythm of conducting Internal Reviews, and the Administrative Decisions Tribunal began delivering considerable guidance on interpretation of the PPIP Act.

The volume of work in this area increased dramatically during 2002-03:

- an 86% increase in the number of new Internal Review matters lodged compared to the previous year
- a quadrupling of the number of privacy matters lodged in the Administrative Decisions Tribunal compared to the previous year.

We responded by developing some new tools to assist both complainants and public sector agencies navigate their way through conducting an Internal Review. Both a standard application form and a ‘checklist’ to assist agencies were launched in April 2003.

The increasing number of ADT matters has unfortunately required the shifting of some resources and focus away from policy and research and into this increasingly complex legal area. However feedback from the Tribunal has suggested our

efforts in assisting the Tribunal members in resolving matters, and providing information about the relevant laws and statutory instruments applicable to each case, are much appreciated. We’ve also started looking at better ways to keep up-to-date with developments in the Tribunal, and elucidate the implications of each ADT decision for both public sector agencies and applicants.

Following the passage of the *Health Records and Information Privacy Act* in the latter half of 2002, we began preparation for its commencement in 2004. One of the differences between the HRIP Act and the PPIP Act which is immediately affecting Privacy NSW is the role of the Privacy Commissioner in issuing statutory guidelines. Unlike what might be called ‘best practice’ guidelines which have no legal force, the statutory guidelines to be issued under the HRIP Act effectively flesh out some areas of the Act, and are legally binding just like other provisions in the Act.

In order to prepare those guidelines prior to commencement of the Act, project funding was obtained from NSW Health under a Memorandum of Agreement, signed in December 2002. In April 2003 two new staff were employed in temporary positions under that funding arrangement, and work began on drafting four statutory guidelines. Those guidelines will be finalised during 2003-04.

INTERNAL REVIEWS

During the reporting year, we were notified of 108 new Internal Review applications, which is almost double that of the previous year. Of the 72 Internal Review applications finalised in the reporting year, 88% were made against State Government agencies. Figure 14 presents respondent agencies categorised by sector.

Like matters which proceeded by way of a Part 4 complaint rather than a Part 5 Internal Review (see the chapter on *Protection of Privacy* in this report), human services dominates as the most likely sector against which privacy complaints

WHAT IS AN INTERNAL REVIEW?

An Internal Review is an internal investigation that a government agency is required to conduct when an individual makes a privacy complaint.

Under Part 5 of the PPIP Act individuals may seek an Internal Review by an agency where they believe there has been 'contravention' of an Information Protection Principle, a Public Register provision of the Act, or a Privacy Code of Practice made under the 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 matters being reviewed or the process of the review.

will be made. However complainants against agencies in the transport sector – most notably the Roads and Traffic Authority – were far more likely to proceed by way of an Internal Review, while complainants against justice agencies were far less likely to do so. This may be because of the significant exemptions for agencies in the justice sector, including exemptions from the IPPs for NSW Police (except in relation to their educative and administrative functions), and exemptions for the judicial functions of courts and tribunals.

In almost half of all matters finalised this year, the Internal Review applicant was a client, customer or patient of the agency (Figure 15). In 15% of matters the applicant was an employee of the agency, a decrease from 23% the previous year.

The most common types of information or practice at issue in Internal Reviews were health records and personal contact details, followed by investigation and law enforcement practices, client / customer records, and identity records (Figure 16). The numbers of applications in relation to criminal records and employment records decreased compared to the previous year.

The most likely Information Protection Principle at issue in an Internal Review was disclosure to a third party, which was included in 60% of all applications (Figure 17). Collection of personal information was part of the conduct reviewed in 18% of cases, and the next most common IPP related to use of personal information.

Figure 14 – Internal Review respondents by sector

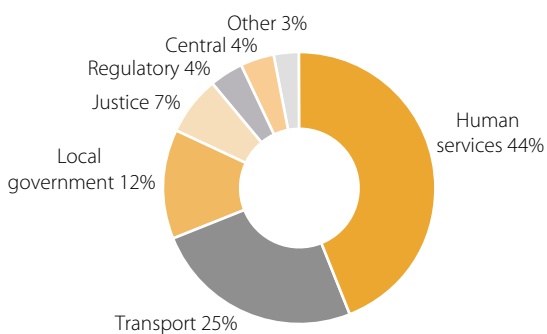
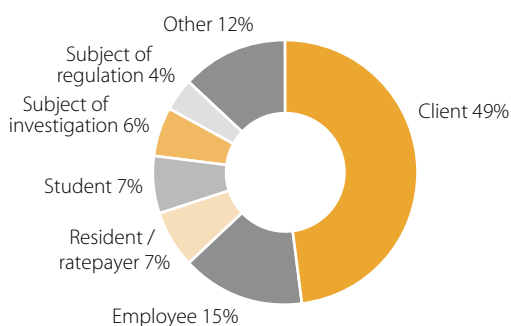


Figure 15 - Relationship of complainant to respondent



Outcome of Internal Reviews

Of the 72 Internal Review files finalised in 2002-03, in 65 cases an Internal Review was completed by the agency concerned. In only one case did the complainant exercise their option of going straight to the Administrative Decisions Tribunal before the Internal Review was complete (i.e. if the review has taken more than 60 days already). A further four applications were withdrawn by the applicant, and in two cases the application was invalid (i.e. it did not allege a breach of any IPP, Public Register provision of the PPIP Act or a Privacy Code of Practice).

Of the 65 reviews completed, a breach of the IPPs was found by the agency in 18 cases (28%).

In terms of outcomes for the 18 cases in which a breach of the IPPs was found, often multiple remedies were offered. The remedies offered to the complainant included apologies (13 cases), rectification (7 cases), and in two cases, financial compensation by way of expenses or damages. There was also systemic change arising from Internal Reviews; in seven cases the outcome included a change in practices in the agency, and in 10 cases re-training of staff was promised as a result.

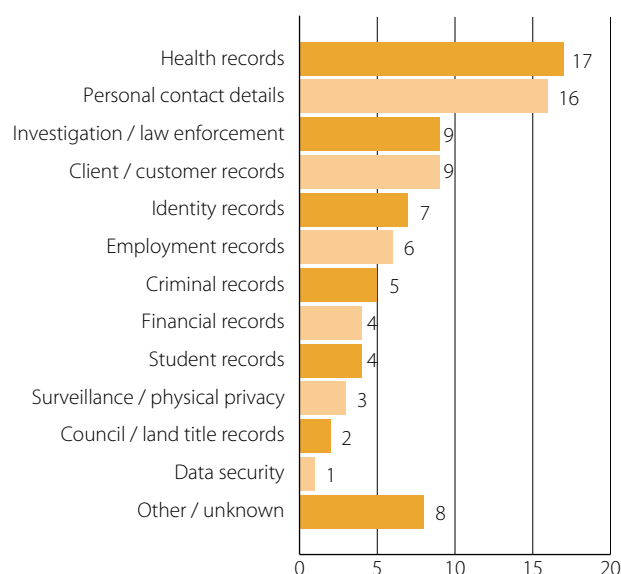
Of the 47 cases where no breach was found, in eight cases the alleged conduct was found never to have occurred, and in 12 cases the evidence was arguable. In 12 cases the conduct was found to have occurred, but the conduct complied with the IPPs. In a further 10 cases the conduct was found to have occurred, it was not in compliance with the IPPs, but nonetheless that non-compliance was authorised by a lawful exemption. Five cases had other reasons for a finding of 'no breach', including findings that the conduct occurred prior to 1 July 2000, or the information at issue was not 'personal information' as defined in the Act.

Privacy NSW oversight role

The quality of Internal Review processes varied greatly between agencies. In order to monitor the situation in a systemic way, in 2002-03 we began collecting statistical data on how much of an input was needed by us to ensure the correct procedure was followed in each case.

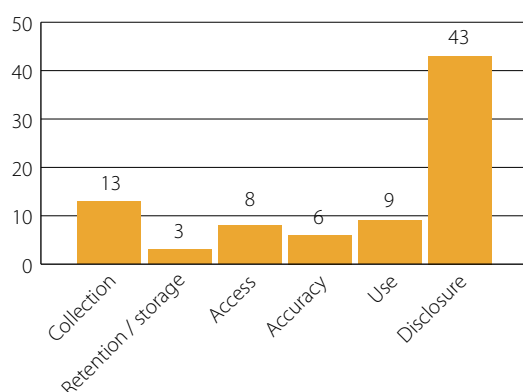
Of the 72 cases seen during 2002-03, 17 (24%) required a significant input from Privacy NSW. The type of input was typically by way of making recommendations about the process or statutory interpretation. In five cases we recommended that the Internal Review findings be revised and reissued to the applicant, because either the findings did not refer to the IPPs in any way (four cases), and / or the findings did not make reference to the applicant's right to appeal to the ADT, as required by the legislation (two cases).

Figure 16 – Internal Review by information / practice*



* The totals reflect the fact that more than one category may be selected for each Internal Review. For the full list of all subject categories see Appendix 3.

Figure 17 - Internal Review by Information Protection Principle(s)*



* The totals in this graph reflect the fact that the conduct or decision subject to an Internal Review may cover more than one IPP. The IPPs are presented in order of information life cycle. This is explained in more detail on page 15, *What do we mean by a Privacy Principle?* However unlike complaints or enquiries, Internal Reviews may only be about the IPPs in the PPIP Act, not any other privacy standards.

Another 25 cases (35%) required a lesser level of input from Privacy NSW, such as reminding the agency of the need to finalise the review (four cases), reminding the agency of the need to progress the review (15 cases), or reminding the agency of the need to notify us of the lodgement of the Internal Review application (six cases).

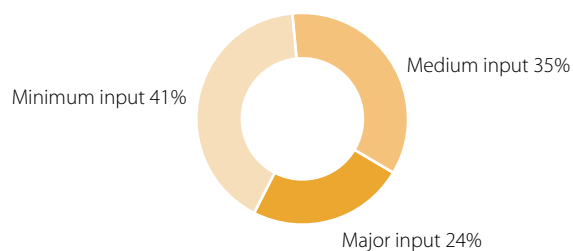
The remaining 30 cases (41%) required little to no input from Privacy NSW, in that we were notified of the Internal Review and we followed its progress without needing to make any submissions to the respondent agency (Figure 18).

In order to make compliance with the procedural aspects of Part 5 of the PPIP Act easier for agencies, we used this type of analysis to develop two tools, both of which were launched in April 2003: a 'checklist' for agencies to follow when conducting an Internal Review, and a template 'application form' for applicants to use. Both of these tools were made available online in Microsoft *Word* format, so as to allow agencies to download the documents and incorporate them into their own forms or templates as required.

Anecdotal evidence suggests that there has been an improvement in the quality of Internal Review processes since we launched the new tools. We hope that the 2003-04 figures will reflect that improvement in comparison to this year's results.

Some of the case studies below demonstrate the manner in which a successful Internal Review process can not only provide a remedy for the individual applicant, but can serve as an important management tool for the agency, in terms of highlighting weaknesses and risk areas that can be addressed to improve compliance across the agency.

Figure 18 – Privacy NSW participation in Internal Reviews



INTERNAL REVIEW CASE STUDIES

THE IMPORTANCE OF BEING NOTIFIED

Ms D attended a public meeting held by her local council about a proposed residential development.

Ms D was unable to stay for the duration of the meeting so made some enquiries of a council employee regarding the development. The council employee advised Ms D that she could leave her name and address for the purpose of receiving a copy of the minutes of the meeting. Ms D did so and noted that the document on which she wrote her name and address included a statement in words to the effect of "please leave your name and address if you would like to receive a copy of the minutes".

She received a copy of the minutes of the meeting titled "Meeting Notes", attached to which was a document titled "From Attendance Lists" which included a list of names and home addresses of all those people who attended the public meeting. The Meeting Notes stated that a consulting company had prepared the minutes and the associated documents. On contacting the consulting firm, Ms D was advised that the firm sent the Meeting Notes to the council, which was then responsible for their circulation.

Ms D was concerned about the circulation of her name and home address to all persons and organisations who received a copy of the Meeting Notes. She lodged an Internal Review with the council with respect to the IPPs relating to collection and disclosure. Ms D noted that if she had been informed of the likely disclosure of her name and home address, she would not have provided her personal details. In particular Ms D was concerned that she would become a target for written material or phone calls from persons in support of, or opposed to, the proposed development.

As part of the Internal Review the council conducted an investigation which included interviews with employees of the consulting firm, the council organisers of the public meeting, and the developers. The council concluded that both the council and the consulting firm had collected names and addresses without providing the required privacy notification of the intended recipients of the information. The council found that it had not collected or disclosed personal information in accordance with the IPPs.

Accordingly the council determined that this information should not be retained in its record system. The council issued an apology to Ms D, and asked the consulting firm to delete the names and addresses of all the resident attendees.

The council also determined that in future such collections must indicate to the public, preferably by means of a notice, the requirement for collecting personal information. The council also noted that there was a lack of understanding of the privacy legislation by council staff, and therefore training in the PPIP Act would be undertaken.

INACCURATE HEALTH RECORDS

Ms E took her baby son to a baby health clinic for a health check up. The clinic was run by the local Area Health Service (AHS).

According to Ms E's Internal Review application, the community nurse who conducted the health check interviewed Ms E and asked whether there was a history of violence between herself and her partner, or within either of their families. When Ms E answered in the negative, the nurse wrote "unknown" next to the question on the assessment form. When asked by Ms E why she wrote this, the nurse said it was because Ms E wouldn't know whether her grandparents had a history of violence. The nurse had not asked a question about

Ms E's grandparents in particular, but only about her family in general.

Ms E then became concerned about the veracity of all the information the nurse had written on the form. She terminated the interview and asked the nurse to hand her the form. The nurse consulted her supervisor who asked Ms E why she wanted the form. Ms E explained that the nurse had made an incorrect notation and she asked the supervisor what would happen if she took the form with her. The supervisor said there would be nothing they could do. Ms E then took the form but the nurse attempted to take the form off her even though Ms E was holding her baby in her arms at the time. The nurse obtained the form and Ms E left the premises.

Ms E sought an Internal Review of the AHS's conduct, in relation to the collection and accuracy of the information collected, and her access and correction rights. The AHS reviewed its conduct by conducting interviews with relevant parties. The Internal Review report concluded that "the form was completed incorrectly" by the nurse and that "there was no attempt to deal with [the] issue in a way that would have allayed the concerns of the client."

The AHS took remedial action including: a formal letter of apology was sent to Ms E; a notation was added to the client file, on the form in question, stating that the initial response was incorrect, and stating what the correct response was; and a copy of the file was provided to Ms E. The AHS also reviewed the template for the form in question, and promised to provide additional instruction to staff in the correct manner of its use. The nurse in question was subject to a disciplinary interview and other adverse action.

The AHS did not agree to Ms E's request that the form be destroyed, on the basis that (i) it would be contrary to various

NSW Health policies that medical records should not be destroyed because they form part of a patient / client history, and (ii) that the document in question was material to the conclusions reached about, and internal action taken against, the nurse involved in the matter.

This Internal Review was exemplary in that the investigation was thorough and the findings clearly written. The report sent to Ms E included extracts of the relevant NSW Health policy documents referred to in the findings. In addition, the report included not only the requisite information about appeal rights to the Administrative Decisions Tribunal, but relevant extracts from the PPIP Act and the ADT's website by way of additional information about that process. The copy of the letter to the applicant was clearly written, and there was a separate letter of apology to Ms E from the Chief Executive Officer of the AHS.

VULNERABLE STUDENT RECORDS

A University student, Ms F, received an email sent to her University email address from Mr G, who was employed by the University in an area dealing with student records. Mr G and Ms F had previously worked together at a different organisation. The email sent by Mr G was not related to University business, and invited Ms F to meet him socially. The email also commented on Ms F's change of name since they had last met.

Ms F alleged that she had not given Mr G her University email address and that he had used University records to make contact with her. She also alleged that Mr G's reference to her previous name suggested that Mr G had had access to her wider student records. Ms F was concerned that this indicated that Mr G might also be able to access her academic marks, financial records, scholarship applications and more sensitive information such as counselling records.

The University conducted an Internal Review and found that Mr G had accessed Ms F's records for the purpose of sending her a personal email message. The University found no evidence that Mr G had accessed or misused any records relating to Ms F other than her University email address. There was no evidence that Mr G obtained access to or misused the records of any other student.

The University concluded Mr G's conduct was such as to cause the University to breach IPP 10, by using personal information for a secondary purpose without lawful authority.

Mr G was also found to have breached the University's Privacy Policy, Code of Conduct, and agreements to protect personal information signed by him when he commenced employment. In misusing information obtained in the course of duty, his conduct also constituted a category of corrupt conduct under the *Independent Commission Against Corruption Act 1988* (ICAC Act).

The University made a formal apology to Ms F, and undertook to implement measures to ensure that the conduct would not occur again. In relation to Mr G, the University directed Mr G not to access any records relating to Ms F, and referred the Internal Review report to the University's Manager of Industrial Relations to determine if any other action ought to be taken against Mr G. The University also undertook to increase its privacy awareness training for staff who have access to student records.

Under IPP 5 of the PPIP Act, agencies are obliged to implement security safeguards to ensure that personal information is protected against loss, unauthorised use, modification, disclosure or other misuse. However as this matter demonstrates, internal policies, staff contracts and IT systems alone cannot eliminate all risk.

This case highlights the increased privacy and corruption risks posed when people have a conflict of interest, such as where agencies engage staff members to deal with records that may relate to their own colleagues, friends or acquaintances. Agencies should be alert to this risk, and take preventive action.

COMPROMISING POSITIONS

This case study also highlights the interrelation between privacy breaches and corruption.

Mr H was a candidate for a position as General Manager of a local council. He was interviewed twice by the selection committee for the council. The selection committee comprised both councillors and community members.

Some time after his second interview Mr H received a telephone call from Mr J. Mr J was a local member of the public, not involved in the recruitment process in any way. Mr J asked Mr H to discuss his job application and performance at interview; Mr H refused. Mr J then sent Mr H a fax in which he made reference to things said by Mr H at interview, and to the panel discussions which followed. Mr J told Mr H in the fax that he wanted Mr H to withdraw his job application, and that if he did not withdraw and was successful, that he would be seen as an "illegitimate ring-in", and that they would "quickly get to know one another quite well".

Mr H withdrew his application for the position. Mr H then received telephone calls from a local journalist, asking about his job application and the lack of confidentiality in the recruitment process.

Mr H made a complaint about a breach of privacy and confidentiality in the manner in which his job application was handled. Mr H alleged that the council had disclosed his name, telephone number and curriculum vitae to Mr J and

possibly to other individuals. He also alleged that the council disclosed information about his performance at interview to Mr J.

The council conducted an Internal Review and identified that Mr H's name, contact details, career history and performance at interview were disclosed by a member of the selection committee to Mr J. However despite interviewing all members of the selection committee, the council could not determine with absolute certainty which individual was responsible for the disclosure. The council attempted to interview Mr J, but without success.

In its findings the council noted the exemption in section 4(3)(j) of the PPIP Act for "information or an opinion about an individual's suitability for appointment or employment as a public sector official". That type of information is not "personal information" for the purposes of the PPIP Act.

The council considered that it was likely that some of the information at issue fell within that exemption, and therefore it could possibly be argued that the conduct relating to some of Mr H's information was not subject to the IPPs. However both the council and Privacy NSW felt that other information – such as an applicant's name and contact details – was probably not of itself "about" a person's suitability for employment, and as such likely fell within the scope of the PPIP Act. (It should be noted that the initial investigation of this question pre-dated any of the case law from the Administrative Decisions Tribunal on this issue.)

Notwithstanding this lack of clarity about the effect of section 4(3)(j) on the conduct under review, the council concluded that the intent of the PPIP Act, particularly IPP 11 with respect to disclosure, had certainly been compromised.

While the council identified the conduct as amounting to a breach of section 664(1) of the *Local Government Act 1993*,

which creates an offence of unauthorised use or disclosure of information, the council could not identify to a sufficient degree the responsible individual against whom a prosecution could be mounted.

Likewise the conduct may have amounted to a breach of section 62 of the PPIP Act, which makes it an offence for a public sector official to disclose personal information otherwise than in connection with their official functions. However this provision would only apply to councillors or employees of the council, not members of the selection committee drawn from community representatives. Furthermore section 62 of the PPIP Act only applies to "personal information", thus again raising the issue of the definitional problem created by section 4(3)(j) of the PPIP Act.

The council concluded that the conduct amounted to corrupt conduct under section 8 of the ICAC Act, and reported it as such to the Independent Commission Against Corruption (ICAC). ICAC advised that they would not pursue the matter, as the complaint had already been referred by the council to the Department of Local Government and Privacy NSW. (It should however be noted that Privacy NSW's involvement was by way of oversight of this Internal Review matter only.)

The council also found that the conduct was a breach of the council's Code of Conduct, but because the responsible individual could not be identified, no disciplinary action could be taken.

The council provided Mr H with a formal apology and a payment of \$5,500 in compensation. This amount reflected the amount that could be paid, by way of fine, by the responsible individual if a breach of section 664 of the *Local Government Act* was proven in court. The council also recommended that all councillors and any existing and future

community members appointed to council committees, working groups or panels, be advised of the council's Code of Conduct and the provisions of the PPIP Act, the ICAC Act, the *Local Government Act* and their relevant penalty provisions. The council also undertook to improve the selection process for senior positions.

This case demonstrates the difficulties associated with the Internal Review process as a forensic exercise, in that officers of an agency conducting an Internal Review do not have any special powers to compel witnesses to appear or give sworn evidence. In this case some witnesses noted their concerns about possible defamatory action arising from any comments they made in recorded interview as part of the Internal Review. This added to their reticence to provide information to the reviewing officer. The council also identified the obvious difficulties facing an officer of an agency who is asked to review the conduct of their superiors or elected members of the council "if they expect to continue working in an organisation".

The PPIP Act makes provision for the Privacy Commissioner to conduct an Internal Review at the request of an agency. However we believe that to do so places Privacy NSW in a position of conflict, given the Privacy Commissioner's additional function of appearing before and assisting the Administrative Decisions Tribunal in its further review of conduct following an Internal Review. Privacy NSW has therefore declined all requests from agencies to conduct Internal Reviews on their behalf.

However we acknowledge the difficulties faced by agencies, in particular small agencies such as local councils, in conducting Internal Reviews. Privacy NSW has suggested to the Attorney General that it may be appropriate to consider an amendment to the PPIP Act, to allow agencies to 'contract out' the conduct of an Internal Review to a suitably qualified and independent body such as an auditor.

This case also demonstrates the unsatisfactory nature of the exemption in section 4(3)(j) of the PPIP Act. What was no doubt intended by Parliament to allow free and frank referee discussions during recruitment processes has instead allowed a free-for-all approach to the misuse of any information, at any time, that could be described as "about" a person's suitability for employment in the public sector. This allows conduct to occur that would otherwise constitute corrupt disclosure under section 62 of the PPIP Act, which carries a maximum penalty of an \$11,000 fine and two years' imprisonment.

WHAT IS PRIVACY NSW'S ROLE IN THE ADT?

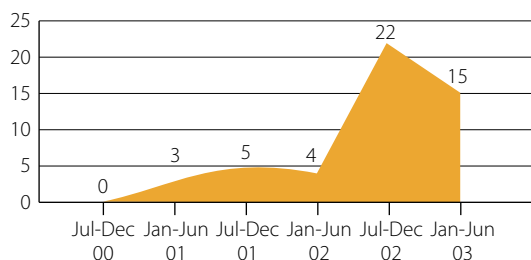
Privacy NSW is notified of applications to the Administrative Decisions Tribunal and has a right to appear and be heard in privacy matters before the Tribunal. The Privacy Commissioner is usually represented by one of Privacy NSW's legal officers. Our role in the Tribunal is primarily concerned with assisting the Tribunal in interpreting the PPIP Act. Our policy is to attend initial 'planning meetings' in the Tribunal to determine whether it may be appropriate to appear in the matter during later proceedings. In accordance with the Commissioner's various functions relating to the protection of privacy, we are concerned that the PPIP Act is interpreted in a way that promotes the objects of the PPIP Act to protect the privacy of individuals. 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.

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 person can apply to the Administrative Decisions Tribunal for a review of the agency's conduct. The Tribunal can review conduct that allegedly breaches an IPP, a Privacy Code of Practice, or a Public Register provision of the PPIP Act. If the Tribunal finds that an agency has breached one of these provisions it can make enforceable orders against the agency. The Tribunal's power to order financial compensation only applies to conduct that occurred after 1 July 2001.

In 2002-03 we were notified of 37 new applications lodged in the Tribunal. This compares with 9 applications lodged in 2001-02 (Figure 19). The Privacy Commissioner's representative appeared at planning meetings in 34 matters. In most cases the parties reached agreement, or the application was withdrawn, dismissed or otherwise not proceeded with. Thirteen matters proceeded to a hearing in 2002-03. We made written and / or oral submissions to the Tribunal in ten cases.

Figure 19 – ADT cases lodged per six months, 2000 to 2003



The Tribunal delivered judgments in eight matters, including one judgment by the Appeal Panel:

24 June 2003	EG v Commissioner of Police [2003] NSWADT 150
4 June 2003	Fitzpatrick v Ambulance Service of NSW [2003] NSWADT 132
30 May 2003	FY v Health Care Complaints Commission [2003] NSWADT 128
16 April 2003	FM v Vice Chancellor, Macquarie University [2003] NSWADT 78
7 April 2003	FH v NSW Department of Corrective Services [2003] NSWADT 72
31 March 2003	DO v University of NSW (GD) [2003] NSWADTAP 9
28 October 2002	DO v University of NSW [2002] NSWADT 211
22 October 2002	Wykanak v Department of Local Government [2002] NSWADT 208

We summarise each new judgment as it comes to hand, and place both the summaries and links to the full judgments on our website.

SECTION 41 DIRECTIONS

In addition to renewing a number of pre-existing section 41 Directions which cover matters currently the subject of the development of more permanent Privacy Codes of Practice, two new section 41 Directions were made during 2002-03.

The *Direction on the Collection of Personal Information from Third Parties by NSW Public Sector Agencies for the ReferralLink Trial* was made on 13 November 2002, in order to facilitate the Better Service Delivery Program. The Better Service Delivery Program is an initiative of the NSW Human Services CEOs Group in partnership with non-government organisations. The Program includes an Electronic Client Referral Project, known as ReferralLink.

The human services agencies identified that IPP 2 caused a difficulty in day-to-day practice. IPP 2 says that information about a person can only be collected from that person.

However, a typical scenario for a human service agency will involve the collection of information from a client about the client's family members, for example whether there is a history of heart disease in that family. This means that the agency is often collecting information about other members of a client's family from the client rather than from the family members themselves.

In order to allow a number of human services agencies to participate in a trial of ReferralLink, a Direction was needed to overcome IPP 2. The Direction was given to enable those agencies to collect personal information about a person indirectly, where the collection of that other person's personal information was reasonably relevant and necessary for the purpose of the agency providing services, diagnosis, treatment or care to their client.

As the ReferralLink trial was extended beyond its original end date of 28 February 2003, the Direction was remade on 28 February 2003, to cover the period until 30 June 2003.

The *Direction on the Collection and Use of Personal Information for the NSW Health Human Tissue Project* was made on 24 February 2003. It is intended to facilitate the collection of personal information by officers of NSW Health and other Health Services for the purpose of consulting with relatives or survivors of deceased people about the disposal of human tissue collected during autopsies. The Direction runs to 1 April 2004.



To empower people to exercise greater control over their personal data, and to encourage NSW public sector agencies to respect the privacy of their clients

KEY RESULT AREA:

Education and Research

One of our core functions as set out in the PPIP Act is to “conduct education programs, and to disseminate information, for the purpose of promoting the protection of privacy of individuals”. This core function is not only part of earmarked ‘education’ activities but is also a key activity in the telephone advice and enquiry service (more detail about the scope of these activities is found in the chapter on *Protection of Privacy*).

During this year, the creation of an Education and Publications Officer position, filled in April 2003, meant that for the first time Privacy NSW has a dedicated officer whose role is to support our core education function. By the end of the financial year, we had our first short-term communications plan approved and implementation began, which is laying the foundation for our first long-term communications strategy. Many new activities, such as the development of a new corporate image, commenced late in 2002-03, and will come to fruition during 2003-04.

In May 2003, staff put “big picture” client service issues under the microscope during a Client Service Skills day. The discussions were lead by a facilitator from the Attorney General’s Department training unit. Staff examined the development of new and additional strategies and functions in order to help Privacy NSW fulfil its core functions, provide better client service and better meet the needs of our various stakeholders.

TRAINING, SPEECHES AND PRESENTATIONS

During this period the Commissioner and staff continued to use speeches, presentations and training opportunities to increase awareness of privacy issues both within the public sector and the wider community. Topics covered during the 21 different presentations during the year were as varied as privacy and access to justice, privacy and ethics, genetics and privacy, and prisoners’ health privacy.

In September 2002, a staff member delivered a training session on “Privacy and Fair Trading” to the Department of Fair Trading. The Deputy Privacy Commissioner was an invited guest speaker at the 2002 International Conference on Personal Data Protection in Seoul, Republic of Korea on 28 November 2002, where she presented a paper on *Electronic Surveillance in the Workplace: Concerns for Employees and Challenges for Privacy Advocates*. In March 2003 the Privacy Commissioner delivered a paper on aspects of genetic privacy at the Privacy Issues Forum, hosted by the New Zealand Privacy Commissioner.



The Deputy Privacy Commissioner, Anna Johnston, speaking in Seoul, Republic of Korea in November 2002.

Other presentations were made to organisations such as:

- Australian Academy of the Humanities – Privacy Roundtable
- State Emergency Management Committee
- NSW Government Lawyers CLE Convention
- AIJA Technology for Justice conference
- AFR Health Congress
- University of Sydney Faculty of Law – Health Law Annual Conference
- Public Health and Human Rights Conference
- FOI and Privacy Practitioners’ Network meetings.



The Hon Justice Michael Kirby, High Court of Australia, Chris Puplick, NSW Privacy Commissioner and Dr Bruce Scoggins, Health Research Council, at the Privacy Issues Forum in New Zealand in March 2003.

OIT PRIVACY AND PERSONAL INFORMATION PROTECTION GUIDELINE

Privacy NSW worked with the Office of Information Technology (OIT) in the development of the *Privacy and Personal Information Protection Guideline*, which was launched by the Privacy Commissioner at a NSW Government forum on 26 July 2002.

The Guideline was developed by OIT (now part of the Department of Commerce) to assist public sector IT professionals, as well as others involved in the informational lifecycle, to understand and implement their obligations under the PPIP Act. The Guideline is in an inter-active format, with active links to the PPIP Act and the latest Government circulars.

This tool is an important step in assisting all public servants ensure that personal information is appropriately collected, stored and used.

At the launch of this Guideline, the Privacy Commissioner also announced a new joint venture between OIT and Privacy NSW, which is an on-line training package about the PPIP Act. The training package was developed jointly with OIT over the course of the year. The package is to be launched in 2003-04.

PUBLICATIONS

Privacy NSW added further to its body of publications during this year, and publications activity is set to increase more dramatically next year, with the position of the Education and Publications Officer recently filled.

One of our most important publications developed this year was the *Draft Guidelines on Consent and Capacity*. The guidelines deal with complex issues that arise in protecting the privacy of adults who may lack “capacity” due to a disability or injury, such as a mental illness, dementia, an intellectual disability, or an acquired brain injury. In developing these guidelines, we are responding to the

need expressed by both members of the public sector and the community to deal with this complex question. This project is also in line with Recommendation No. 34 of the NSW Legislative Council Select Committee on Mental Health's *Inquiry into Mental Health Services in New South Wales*, Final Report, December 2002. The guidelines were made available for public consultation in April 2003 and were the subject of a consultation evening in May (see *Partnerships and Consultation* in this report for more about that event).

We also continued the series of Privacy Contact Officer newsletters, with an edition in April 2003 sent out to all public sector agencies and also made available on our website. The newsletter provided information on new cases in the Administrative Decisions Tribunal, new tools to assist in the conduct of Internal Reviews, and other emerging issues.

Two of our most popular publications this year were tools developed to assist public sector agencies and members of the public in carrying out Internal Reviews. The first tool is a checklist to help public sector agencies conduct Internal Reviews, which was made available via our website. This is a much more comprehensive version of the checklist from our 1999 guidelines. It includes cross-references to the PPIP Act, helpful advice on process based on ADT judgments to date, and tips from our experience of overseeing the 176 Internal Reviews lodged since the PPIP Act commenced.

The second tool is a standardised Internal Review 'application form', whose purpose is not only to help complainants formulate their applications, but also to assist public sector agencies in dealing with Internal Reviews. The application form was also made available via our website. We have already received positive feedback about both these tools and are seeing them used in a growing number of Internal Reviews.

We also continued to distribute our earlier series of guidelines on the PPIP Act (see Appendix 2).

PRIVACY NSW ON-LINE



We continued to maintain our website which is part of the Lawlink NSW website hosted by the NSW Attorney General's Department.

The website continues to be our most important medium for the publication of guidelines, recent news, practical privacy tools and case summaries from the Administrative Decisions Tribunal. Towards the end of the year, we began a benchmarking exercise in order to prepare for a new website template, which is to be rolled-out in 2003-04.



To build mutually beneficial
partnerships with clients,
stakeholders and other privacy
agencies

Consultation and Partnerships

As the scope and nature of privacy issues in society broadens each year, we have responded to growing demands to participate in discussions and debates on a variety of issues. We formed partnerships and consulted with the community on these matters, including in new fields not previously tackled by Privacy NSW.

We built on existing consultation groups and partnerships, with continued participation in PANZA+ and in convening meetings for the Privacy Advisory Committee and the Privacy Roundtable (see below). We also strengthened our network of Privacy Contact Officers through our participation in the quarterly FOI & Privacy Practitioners' Network meetings and through regular information bulletins.

PARTICIPATION IN WORKING PARTIES

Staff participated in a wide variety of working parties during this period. These included:

- The Inter-agency Working Party on Identity Theft
- The Inter-agency Working Party on the Alcohol Interlock Project
- The Inter-departmental Committee on Closed Circuit Television (CCTV)
- The Working Party on the Implementation of the *Child Protection (Registration of Offenders) Act 2000*
- The NSW Chronic Care Personal Health Records Steering Committee
- The NSW Electronic Health Record Steering Committee
- The NSW Innocence Panel
- The Oversight Committee for Division of Analytical Laboratories (DNA Laboratories).

The Commissioner also gave evidence at two Parliamentary Inquiries:

- The NSW Legislative Committee Select Committee on Mental Health - *Inquiry into Mental Health Services in New South Wales*
- The Australian Parliamentary Joint Committee on the National Crime Authority – review of the *Australian Crime Commission Establishment Bill 2002*.

CONSULTATION ON CONSENT AND CAPACITY GUIDELINES

Privacy NSW took advantage of Law Week to open its doors on 15 May 2003 to a diverse group of stakeholders to discuss the *Draft Guidelines on Consent and Capacity*.

The consultation forum was opened by Julie Baker, Assistant Director-General of the NSW Attorney General's Department, and introduced by Maureen Tangney, Acting Privacy Commissioner. The draft guidelines were welcomed as an important initiative by speakers Phillip French from People With Disabilities and John Le Breton from the Office of the Public Guardian.

Approximately 50 people attended, including representatives of public sector agencies, consumers representing advocacy and self-help organisations, carers, non-government service-providers, and members of the health and legal professions.

The consultation was highly interactive and facilitated by an independent moderator, with the assistance of trained facilitators from the Attorney General's Department training unit. The technique used featured:

- Visual: participants' contributions were visualised on a series of 13 large pin boards covering key issues from the draft guidelines;
- Active participation: everybody was able to have a 'say' in group discussions and / or with the use of visual discussion tools (coloured cards, stickers, etc) on the pin boards;

- Choice of focus: participants were able to move around the pin boards and focus on issues that they felt most strongly about, without pressure to contribute on other matters.

Participants were asked to comment about the key issues in terms of what works, what doesn't work, and what are the challenges. A hypothetical scenario about 'Dorothy', a woman living with schizophrenia and dementia, was also displayed on the pin boards. Participants could use the scenario and / or their own experiences to stimulate discussion.

A wealth of feedback was obtained from participants on the draft guidelines using this lively method. Participants were overwhelmingly positive about both the need for the guidelines and the interactive nature of the consultation itself.



From left to right: Phillip French, Executive Officer, People With Disabilities, Maureen Tangney, Acting Privacy Commissioner, Julie Baker, Assistant Director-General, Attorney General's Department, and John Le Breton, Director, Office of the Public Guardian at the Law Week consultation.



An officer of Privacy NSW demonstrates how to use the interactive pin boards.

PRIVACY AGENCIES OF NEW ZEALAND AND AUSTRALIA (PANZA+)

Privacy Agencies of New Zealand and Australia (PANZA+) is a forum for the discussion of a range of privacy related matters. PANZA+ is an opportunity to form partnerships and exchange ideas about privacy regulation, new technologies and the management of privacy enquiries and complaints. Privacy NSW hosted the PANZA+ meeting of November 2002 in Sydney. Representatives from Privacy Victoria, the Office of the Australian Federal Privacy Commissioner, the Office of the New Zealand Privacy Commissioner and the Office of Hong Kong Privacy Commissioner attended the meeting on the first day. On the second day, this group was expanded to include representatives from other Australian State jurisdictions concerned with privacy issues but without an independent statutory Privacy Commissioner.

Apart from jurisdiction reports presented by each represented agency, items discussed included the current international consultation on the World Anti-Doping Code, cross-jurisdictional law enforcement, new laws on privacy,

and methodologies for reporting and publishing privacy decisions.

PANZA+ convened for a second time this reporting year in March 2003 in Wellington, New Zealand. Items discussed included identity cards, new legislation such as health records privacy and anti-SPAM, the rights of prisoners and complaints handling.

PRIVACY ADVISORY COMMITTEE

Part 7 of the PPIP Act provides for a Privacy Advisory Committee, whose functions are:

- a) to advise on matters relevant to the Privacy Commissioner's functions
- b) to recommend material to the Privacy Commissioner to be included in guidelines
- c) to advise the Minister on matters referred to it by the Minister.

The Privacy Commissioner chairs the meetings of the Committee. The Committee consists of up to six members, two from the Parliament of NSW (representing both the Government and the Opposition) and others with a special knowledge of or interest in privacy matters.

As at 1 July 2002 the members of the Privacy Advisory Committee were:

- Professor Joan Cooper, University of Wollongong
- Ms Mary Bolt
- Mr Bill Grant, Chief Executive, Legal Aid Commission
- Ms Alison Peters, NSW Labor Council
- Mrs Barbara Perry MP (representing the Government)
- Hon Jim Samios, MLC (representing the Opposition).

The Hon Jim Samios MLC retired at the State election in March 2003. Professor Cooper resigned from the Committee in June 2003.


The Committee met four times during this period, on 12 September and 13 December 2002, and on 13 March and 12 June 2003. Items discussed during these meetings covered both on-going matters, updates on legislation and a review of our work. During the year, some of the major topics discussed included progress on the Health Records and Information Privacy Bill, progress on the NSW Law Reform Commission's report on surveillance, the Australian Law Reform Commission's review of the protection of genetic information, new ADT cases, communications with stakeholders and the progress on the implementation of our organisational restructure.

PRIVACY ROUNDTABLE

The Privacy Roundtable was established in the year 2000 by the Privacy Commissioner to act as a stakeholder forum for discussion of privacy issues, to provide feedback on how those issues are considered within different sectors of the community, and to act as a sounding board for policy proposals and research projects.

Membership of the Roundtable is drawn from privacy contact officers in public sector agencies, as well as business, consumer, public interest and privacy advocates.

The Roundtable met four times this reporting year, in August and November 2002, and February and May 2003. During these meetings, Roundtable members discussed upcoming privacy issues and also reviewed current work being carried out by Privacy NSW. The meetings continued to be an excellent forum for the workshopping of ideas from a wide spectrum of viewpoints.

A woman with curly hair, wearing a white lab coat, is seated at a desk in a bright office. She is looking towards a laptop screen. The desk has a white mug and some papers. A large window with a grid pattern is in the background. A decorative pattern of white circles and squares is overlaid on the right side of the image.

To ensure that the administrative framework of Privacy NSW supports all officers in their work, and that the skills and talents of staff are utilised in the workplace

Administration and Staff Development

A number of significant developments during 2002-03 have substantially reformed the operations of Privacy NSW. This was to address the primary finding of an independent review in 2001-02: that Privacy NSW had “a reactive, rather than proactive, approach to privacy management”

ORGANISATIONAL RESTRUCTURE AND GROWTH

During 2001-02 the Attorney General's Department funded an independent resourcing review of Privacy NSW (the Andersen review). The results of that review were detailed in our 2001-02 Annual Report. The recommendations arising included an organisational restructure, and a budget increase sufficient to expand our office from six to ten full-time staff.

The Attorney General's Department responded by increasing the budget allocation for 2002-03 to \$861,000, up 42% from \$607,000 in 2001-02. Of this increase, the amount of \$105,000 related to employee-related payments (that is, for new staff), while the remainder related to increased operational expenses (most notably rental increases).

We implemented the new organisational structure recommended by the Andersen review, by reorganising the supervisory and workflow structure into four functionally based teams:

- Legal, Policy & Research
- Compliance & Investigations
- Education & Publications
- Office Management

We also created four new positions:

- Senior Legal & Policy Officer
- Senior Compliance & Investigations Officer
- Education & Publications Officer
- Correspondence Manager

These four new positions were filled between January and April 2003. However the budget increase was not sufficient to maintain a permanent staffing of ten officers, and so two existing positions remain effectively vacant.

In order to prepare for the introduction of the HRIP Act, funding was also obtained from NSW Health under a Memorandum of Agreement, signed in December 2002, for several pre-commencement projects. In April 2003 two new staff were employed in temporary positions under that funding arrangement.

In May 2003 there was a change of Privacy Commissioner, following the resignation of Chris Puplick after more than four years in the position. Chris had joined the then NSW Privacy Committee on 11 November 1992. He was made Chair of the Committee on 2 June 1993, and was appointed as inaugural Privacy Commissioner of New South Wales from the commencement of the PPIP Act on 1 February 1999. Chris resigned effective from 2 May 2003.

Ms Maureen Tangney was appointed as Acting Privacy Commissioner by the Attorney General for a period of three months from 3 May 2003. Maureen had previously been Executive Member of the NSW Privacy Committee, and is currently Director, Legislation & Policy, in the NSW Attorney General's Department.

As at 30 June 2003, in addition to Acting Commissioner Maureen Tangney, Privacy NSW had ten staff, filling eight permanent and two temporary positions:

- Anna Johnston, Deputy Privacy Commissioner

Legal, Policy & Research team

- John Gaudin, Senior Legal & Policy Officer
- Lucy Blamey, Legal & Policy Officer
- Natasha Mann, Legal & Policy Officer (HRIP Act)
- Michelle Johnson, Policy & Research Officer (HRIP Act)

Compliance & Investigations team

- Siobhan Jenner, Senior Compliance & Investigations Officer
- Jacqueline Roarty, Investigations Officer

Education & Publications team

- Leila Loupis, Education & Publications Officer

Office Management team

- Rosemarie McEwan, Correspondence Manager
- Peggy Phan, Office Manager

MAJOR IT REFORM PROJECT

In May 2003 the Attorney General's Department approved additional capital works funding for the development of a comprehensive new IT system for Privacy NSW. The purpose of the system is to better manage our file-based work (complaints, advices, Internal Review oversight, appearances in the Administrative Decisions Tribunal and so on), our enquiries work, and our educational and research resources. Its core objective is to improve individual work management and group project management.

The project commenced immediately once funding was approved, as we were able to build upon earlier projects to develop comprehensive subject keywords, and map our existing business rules. Enovate Consulting Pty Ltd was contracted by the Attorney General's Department to develop the new system, to be called PRISM - the Privacy Records and Information System.

By 30 June 2003 work was well underway towards finalising the full specifications, and a very early prototype had been developed. We expect that work on PRISM will be concluded in 2003-04.

From 1 July 2002 our enquiries database was revised to incorporate the new comprehensive subject keywords mentioned above, so as to bring the enquiries service into line with the systems developed in 2001-02 for file-based work. This has enabled better analysis of emerging trends, and uniform reporting so as to allow better comparison across different areas of our work, as well as the work of other Privacy Commissioners in comparable jurisdictions. The results in terms of reporting are evidenced in this Annual Report.

We also developed an interim database with which our Legal, Policy & Research team could track the progression of privacy matters in the Administrative Decisions Tribunal.

Each of these systems will be further improved as they are incorporated into PRISM.

CLIENT SERVICE DELIVERY

In 2002-03 we built upon initiatives which had begun the previous year to improve our client service. Key to improving our client service is improving our communications. While many of the education and training oriented initiatives commenced during this period will not be evidenced until 2003-04, a number of new tools were launched during 2002-03. These included an Internal Review 'checklist' for public sector agencies, and an Internal Review 'application form' for members of the public.

Transparency about how we deal with privacy complaints is an important aspect of client service. During 2002-03 our Complaints Protocol was extensively revised, and published on our website, as were details of a new arrangement under which complaints may be transferred (with the complainant's express consent) between our Office and other statutory bodies in New South Wales such as the Health Care Complaints Commission and the Anti-Discrimination Board (see page 25 of this report).

The Flexible Service Delivery Team, comprising one officer from Privacy NSW and two officers from the Anti-Discrimination Board, held a community consultation in June 2002, which identified key objectives including:

- improved physical access to and safety within 201 Elizabeth Street for people with disabilities
- availability of information and publications in suitable formats
- improved access to enquiries and complaints-handling services
- raising staff awareness about issues affecting people with disabilities.

The team's recommendations, implemented in 2002-03, included:

- access audit of premises at 201 Elizabeth Street by expert disability consultant
- audit of format of Privacy NSW publications
- relocation of TTY to improve access and staff training in the use of TTY
- development of visual and word maps for 201 Elizabeth Street
- development of a resource database on disability issues for staff.

CORPORATE SERVICES

During 2002-03 we implemented a file disposal and archiving strategy to deal with old Privacy Committee files dating back to 1975. We also began development of a Privacy NSW Disposal Authority, necessary under the *State Records Act* in order to deal with records created since 1999 when Privacy NSW came into existence.

Other corporate services projects included the development of our own Privacy Management Plan (distinct from the Attorney General's Department's Plan), a Conflict of Interest Policy and Conflict of Interest Register, and we commenced work on a Media / Public Speaking Protocol.

STAFF DEVELOPMENT AND TRAINING

Following the appointment of the new team leaders (Senior Legal & Policy Officer and Senior Compliance & Investigations Officer), management training was offered. One officer commenced the Public Sector Management Program, while the other completed the IPAA course on 'managing teams effectively' during 2002-03, and will commence the Public Sector Management Program during 2003-04.

Other officers attended courses including Skillmax English grammar and writing, in-house Attorney General's Department courses on developing and writing operational policy and procedures, effective communication, media management, conflict resolution, and client service skills training. A number of health privacy specific training and conference opportunities were made available for the new officers working towards implementation of the HRIP Act, and two officers attended the NSW Investigations Symposium.

With the assistance of the Attorney General's Department we also developed and held a very successful training day for all staff in May 2003, focusing on the specific client service skills necessary for Privacy NSW staff.

Also during 2002-03 the Deputy Privacy Commissioner was appointed to the Attorney General's Department Executive Development Advisory Committee, to work on staff development issues across the Department.

Appendix

APPENDIX 1 – FINANCIAL STATEMENTS 2002–03

	ACTUAL \$	BUDGET \$
TOTAL REVENUE	5,087	0
EXPENSES		
Total Employee Related Payments	589,724	594,789
Total Maintenance & Working	275,442	322,164
Total Depreciation	3,405	4,331
Total Other Services	960	0
TOTAL EXPENSES	869,531	921,284
Less: Revenue	(5,087)	0
NET COST OF SERVICES	864,443	921,284
Less: Depreciation – Plan & Equipment	(3,405)	(4,331)
Less: Crown Liabilities	(74,685)	(54,235)
NET POSITION	786,353	862,718

APPENDIX 2 – PUBLICATIONS AVAILABLE FROM PRIVACY NSW

<i>Privacy and Personal Information Protection Act: A Plain English Guide</i>	\$5.50
A Guide to Making Privacy Codes of Practice (1999)	\$5.50
A Guide to Making Privacy Management Plans (1999)	\$5.50
A Guide to Internal Reviews (2000)	\$5.50
A Guide to Public Registers (2000)	\$5.50
A Guide to the Information Protection Principles (2000)	\$8.00
Privacy NSW Annual Report 1998–1999	No charge
Privacy NSW Annual Report 1999–2000	No charge
Privacy NSW Annual Report 2000–01	No charge
Privacy NSW Annual Report 2001–02	No charge

*Some publications of the former Privacy Committee are also available.
Please contact Privacy NSW for details.*

APPENDIX 3 – CATEGORIES OF INFORMATION OR PRACTICE AT ISSUE

This table sets out the full set of categories by which advice, enquiries, complaints and Internal Review matters are coded.

<p>Biometric / Physical information</p> <ul style="list-style-type: none"> – DNA / genetics <ul style="list-style-type: none"> • Identity • Kinship • Medical – Fingerprints / palm prints – Facial recognition – Voice recognition – Iris / retina scanning – Drug / Alcohol testing – Psychological testing – Human tissue / organs – Other <p>Search / Seizure</p> <ul style="list-style-type: none"> – Search of <ul style="list-style-type: none"> • Body • Bag / locker / desk / possessions • Vehicle • Building – Search by <ul style="list-style-type: none"> • Sniffer dog • Person • Screening equipment <p>Surveillance / Monitoring / Physical privacy</p> <ul style="list-style-type: none"> – Video / CCTV – Listening device – Email / Internet monitoring – Performance monitoring – Smart card / Credit card monitoring – Location positioning <ul style="list-style-type: none"> • Vehicle tracking • Mobile phone positioning • GPS / GIS / Satellite devices • Other – Mail – interception / interference / monitoring – Telecommunication – interception / interference / monitoring – Photographs – taking / publishing – Building proximity – Trespass – Stalking / Harassment – Other 	<p>Advertising / Direct marketing / Mailing lists / SPAM</p> <ul style="list-style-type: none"> – Mail – Email – Telephone calls – Door-knocking <p>Auditing / Consulting</p> <p>Credit / Banking / Financial / Tax records</p> <p>Criminal histories / Driving records</p> <ul style="list-style-type: none"> – Criminal history / COPS event / Arrest / Charge / Intelligence <ul style="list-style-type: none"> • Child protection related • Not child protection related • Both • Unknown – Criminal record <ul style="list-style-type: none"> • Child protection related • Not child protection related • Both • Unknown – Spent conviction <ul style="list-style-type: none"> • Child protection related • Not child protection related • Both • Unknown – Driving infringement record – Other <p>Court / Tribunal activities</p> <ul style="list-style-type: none"> – Court lists – Court records – Process serving – Judgments – Conduct of hearing <p>Customer / Membership records</p> <p>Data security / Storage / Archiving</p> <p>Debt collection</p> <p>Electoral rolls</p> <p>Employment records</p> <p>Family / Community history (genealogy) records</p> <ul style="list-style-type: none"> – Births, deaths, marriages – Adoption – Foster care – State wards 	<p>Identity / Age records / Identity theft</p> <ul style="list-style-type: none"> – Identity as a complainant / informant – Drivers license – Passport – Birth certificates / Birth cards – Proof of age documents – Medicare card – ID cards – Unique identifiers / Data matching – Identity theft – Other <p>Investigation / Law enforcement practices / Inquiries</p> <ul style="list-style-type: none"> – By law enforcement officials – Investigation by others – Commissions & Inquiries <p>Land title / Local council records</p> <ul style="list-style-type: none"> – Land title records – Rates records – Development application records – All council records – Other <p>Medical / Health records</p> <ul style="list-style-type: none"> – Genetic health – Mental health – Sexual health – Drug / alcohol use / abuse – All health – Other <p>Personal contact details</p> <ul style="list-style-type: none"> – Name – Address – Telephone number <ul style="list-style-type: none"> • Unlisted • Listed • Unknown – Email address – Other <p>Student records</p> <p>Surveys / Research / Census</p> <p>Tenancy information</p> <p>All records / practices</p> <p>Other</p> <p>Unknown</p>
---	---	--

APPENDIX 4 – GLOSSARY OF TERMS

ADT	Administrative Decisions Tribunal
AHEC	Australian Health Ethics Committee, part of the NHMRC
AHS	Area Health Service
ALRC	Australian Law Reform Commission
DPP	Data Protection Principle
FOI	Freedom of Information
HPP	Health Privacy Principle
HRIP Act	<i>Health Records and Information Privacy Act 2002</i>
IPP	Information Protection Principle
NHMRC	National Health and Medical Research Council
OIT	Office of Information Technology, now part of the Department of Commerce
PANZA+	Privacy Agencies of New Zealand, Australia and Hong Kong
PIIP Act	<i>Privacy and Personal Information Protection Act 1998</i>
PIIP Regulation	Privacy and Personal Information Protection Regulation 2000



Privacy NSW

Office of the NSW Privacy Commissioner

PO Box A123, Sydney South NSW 1235

Level 17, 201 Elizabeth Street, Sydney NSW 2000

Phone (02) 9268 5588

Fax (02) 9268 5501

TTY (02) 9268 5522

www.lawlink.nsw.gov.au/privacynsw

ISSN 1448-4609

© Privacy NSW 2004