

Annual Report 1999-2000



PRIVACY
NEW SOUTH WALES

Privacy NSW is the Office of the NSW Privacy Commissioner, established under the *Privacy and Personal Information Protection Act 1998*. The role of Privacy NSW is to educate people about privacy issues and to ensure that the people of NSW have their privacy rights respected.

The Hon R J Debus, MP
Attorney General
Level 20,
Goodsell Building
8-12 Chifley Square
SYDNEY 2000

Dear Mr Debus

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 1999/2000.

Yours sincerely

A handwritten signature in black ink, appearing to read "Chris Puplick". The signature is stylized and written over a faint, light-colored circular stamp or watermark.

Chris Puplick
Privacy Commissioner



About Privacy NSW

Privacy NSW is the Office of the NSW Privacy Commissioner, established 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; and
- ▶ 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 education the community about privacy issues; and
- ▶ by advising people of possible remedies for breaches of their privacy and by receiving, investigating and conciliating complaints about breaches of privacy.

Contents

| | |
|--|-----------|
| Commissioner's Message | 2 |
| Introduction | 4 |
| Legislative Framework | 7 |
| Introduction | 7 |
| Application of Legislation to the Private Sector | 7 |
| Commencement of the Legislation | 7 |
| The Privacy & Personal Information Protection Regulation 2000 | 8 |
| Privacy Management Plans | 8 |
| Privacy Codes of Practice | 9 |
| Protection of Privacy | 11 |
| Telephone Queries | 11 |
| Complaints | 12 |
| Legislative Changes and the Complaints Process | 14 |
| Complaint Case Studies | 15 |
| Advice | 18 |
| Advice Case Studies | 19 |
| Research | 21 |
| Flashback: How have issues changed in the past 10 years? | 22 |
| Education | 27 |
| Consultation and Partnerships | 29 |
| Privacy Agencies of Australia and New Zealand (PANZA) | 29 |
| Consultation on the Privacy Amendment (Private Sector) Bill 2000 | 29 |
| Privacy Advisory Committee | 31 |
| Administration | 33 |
| Staffing | 33 |
| Financial Statements | 34 |
| Publications | 36 |



No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Universal Declaration of Human Rights, 1948

COMMISSIONER'S MESSAGE



The last year of the Twentieth Century, like all *fin de siècle* periods, saw much reflection upon the nature of our society - how it had changed in the previous century and what lay ahead in the next. Much of this discussion focused upon such issues as the continuing relevance and role of government in our lives; the impact of new technologies and the prospects of the next century being one in which the genetic revolution would rewrite many of the rules of the game. Throughout such discussions and speculations, the rights of individuals to have their privacy and autonomy respected and protected ran like a constant golden thread.

During this last year in New South Wales we have been able to conduct this debate against a background of the gradual implementation of a specific piece of legislation designed to protect and enhance the privacy of individuals. For all of its many weaknesses, themselves the result of the inevitable compromises upon which the democratic political process relies, the *Privacy and Personal Information Protection Act 1998* is the first attempt by any State Parliament to start to grapple with these difficult issues.

It has been my challenge and that of my officers at Privacy NSW to start to make this piece of legislation work and to prove its value to the people of this State.

Apart from being responsible for the actual administration of the legislation I see my role as the State's first Privacy Commissioner to have three key elements relating to privacy and its protection and enhancement : to identify issues in

the current climate; to anticipate issues likely to arise in the foreseeable future and to educate the community about such issues.

The identification of current issues is relatively straightforward. My 1999/2000 Report provides details about the issues which have been dealt with by my Office in the last year. It also reflects upon how many of these issues were on the agenda of the previous Privacy Committee of New South Wales ten years ago.

Anticipating issues is more difficult and requires Privacy NSW to keep a very wide watching brief. I have no doubt that the promises and threats of the genetic revolution will be one of the great areas of social debate over the next decade. This debate will touch upon issues related to the very fundamental questions of how we create life, how we perceive ourselves as human beings and what role we see our governments as having in regulating and adjudicating impossibly conflicting

“This is a free country, madam. We have a right to share your privacy in a public place.”

Sir Peter Ustinov : “Romanoff and Juliet” (1956) Act 1

claims. Within this discourse privacy will be a central issue. Similarly the changing nature of personal and business communications will confront us with challenges - the personal conversations which were once private are yielding to the email communications which are not private; the security of our financial records once kept closely guarded are now broadcast on the internet; even the details of what may be found in our supermarket shopping trolley, once barely noticed are now minutely recorded. It is a key role of my Office to ensure that all these developments are monitored. We are not the office of King Canute and cannot roll back some of the tides, but we can shape how they flow and whether or not they are allowed to erode the shores of our personal privacy.

As part of my educative function during the course of this year I made over fifty presentations about privacy

issues to groups as diverse as business leaders; Company and Chartered Secretaries; departmental Privacy Contact Officers; investigative agencies; conferences of Judges; University ethics committees; workers in the child protection area; representatives of the gambling industry; medical practitioners and researchers and planners for the Sydney Olympic Games. I also participated in numerous working parties and committees within the structures of the State Government and at the end of the year was appointed to head a Committee of Enquiry examining the proposal to introduce a system of linked personal electronic health records throughout the State.

The year ahead will be equally challenging – identifying the weaknesses of our legislation (for example the non-coverage of State owned corporations) – working with our federal colleagues whose new

Act will impact significantly on our activities – and maintaining our level of service to the people of this State.

I would like to conclude by thanking all my staff, the Attorney General and the Director General of his Department for their support and encouragement and to assure them all that as Commissioner I am looking forward to the challenges of the next few years with eager anticipation.



Chris Puplick
NSW Privacy Commissioner

INTRODUCTION

PRIVACY NSW AS PART OF THE ATTORNEY GENERAL'S DEPARTMENT

The Attorney General's Department of NSW administers the NSW legal system, and implements programs to promote a safe and harmonious society. It is the vision of the Department to ensure that:

The rights of the people of NSW are promoted and protected and their responsibilities are understood and accepted.

The Attorney General's Department is made up of 39 business units which operate independently of each other. As the roles of the business units are diverse, the Department has grouped the units into programs to focus operations and planning. Privacy NSW is part of the Human Rights program, which aims to ensure the individual rights of the people of NSW are understood and respected.

The corporate goals of the Attorney General's Department are to:

1. Continuously improve our services and increase satisfaction among our diverse clients.
2. Promote the earliest, most effective and efficient resolution of criminal matters and civil disputes.
3. Contribute to the development of a legal system and laws in NSW that further the principles of justice and contribute to the achievement of the goals of the Government.
4. Reduce social disharmony through programs which prevent crime and protect human rights.
5. Build a harmonious organisation which reflects the diversity of the people of NSW.

Privacy NSW plays a fundamental role in contributing to the vision and corporate goals of the Attorney General's Department. The key result areas of Privacy NSW highlight how this was achieved in 1999/2000.

1999/2000 KEY RESULT AREAS AND ACHIEVEMENTS

The achievements of Privacy NSW for each key result area in the reporting period include:

| <i>Key Result Area</i> | <i>Achievements</i> |
|--|---|
| <p>LEGISLATIVE FRAMEWORK</p> <p>To ensure that NSW public sector agencies are aware of and comply with the requirements of the Act</p> | <ul style="list-style-type: none"> ▶ assisting agencies in the development of privacy management plans; ▶ advising on the <i>Privacy and Personal Information Protection Regulation 2000</i>; ▶ submitting recommendations to the Attorney General on the privacy code of practice for the NSW Public Sector Workforce Profile; |
| <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"> ▶ responding to over 2000 telephone enquiries of which more than 70 per cent received immediate advice or information; ▶ closing over 170 complaint files, with more than 76 per cent being conciliated or resolved; |
| <p>EDUCATION</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"> ▶ hosting the inaugural meeting of privacy contact officers to provide information and advice concerning new legislative requirements; ▶ developing and delivering a series of training sessions to outline the responsibilities of agencies under the Act; ▶ publishing a series of plain English guidelines to provide further guidance on compliance with the Act; ▶ maintaining and updating information on the Lawlink website about privacy legislation and the functions of the Privacy Commissioner; |
| <p>CONSULTATION AND PARTNERSHIPS</p> <p>To build mutually beneficial partnerships with clients, stakeholders and other privacy agencies</p> | <ul style="list-style-type: none"> ▶ attending the Privacy Agencies of New Zealand and Australia (PANZA) forum to discuss and provide input into a range of privacy related matters; ▶ participating in consultation with the federal Attorney General's Department concerning proposed federal privacy legislation to apply to the private sector; |
| <p>ADMINISTRATION</p> <p>To ensure that the administrative framework of Privacy NSW supports all officers in their work</p> | <ul style="list-style-type: none"> ▶ moving premises to co-locate with the Anti-Discrimination Board; and ▶ reviewing the Privacy NSW staff structure to better meet the requirements of the new legislation. |



To ensure that NSW public sector agencies are aware of and comply with the requirements of the Privacy and Personal Information Protection Act 1998

KEY RESULT AREA:

Legislative Framework

INTRODUCTION

The *Privacy and Personal Information Protection Act 1998* has two principal purposes. First, it sets up the Office of the Privacy Commissioner, and gives the Commissioner powers which were held in the past by the Privacy Committee. These include the power to conduct research, provide advice and handle complaints about breaches of privacy. Secondly, the Act introduces the Information Protection Principles, a set of privacy standards which regulate the way most NSW public sector agencies deal with personal information.

Under section 3 of the Act, public sector agencies include:

- ▶ government departments;
- ▶ the Education Teaching service;
- ▶ a statutory body representing the crown;
- ▶ a declared authority under the *Public Sector Management Act 1988*;
- ▶ the NSW Police Service; and
- ▶ local councils.

State owned corporations are excluded from the definition, and the Act excludes the judicial functions of courts and tribunals from any obligations arising under the Act.

APPLICATION OF THE LEGISLATION TO THE PRIVATE SECTOR

While the Act only provides legal remedies in relation to privacy breaches by public sector agencies, it also gives the Privacy Commissioner the power to investigate and conciliate complaints about breaches of privacy by organisations that are not public sector agencies. The Privacy Commissioner has adopted the Privacy Committee's Data Protection Principles as the standard for determining such information privacy complaints.

WHAT IS PRIVACY?

There is no simple definition of privacy to cover all circumstances. A number of elements may be considered, including such things 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 focussing on the need to ensure the fair use of information. The fair use of 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.

COMMENCEMENT OF THE LEGISLATION

As reported in 1998/99, the Act commenced in stages from 1 February 1999 when the Privacy Commissioner took over the functions of the Privacy Committee, and the *Privacy Committee Act 1975* was partly repealed. From 1 June 1999 the Privacy Commissioner began to exercise functions under the new Act to investigate complaints, advise on compliance with the Act and recommend privacy codes of practice to the Attorney General for approval.

Part 3, Division 2 commenced on 1 July 1999. This Part required public sector agencies to prepare privacy management plans over the next twelve months. At the same time sections 62 and 63 of the Act introduced penalties for corrupt or improper disclosure, or trafficking in, personal information. In late 1999 and early 2000, Privacy NSW conducted training sessions for agencies on the preparation of privacy management plans and codes.

From 1 July 2000 the Act will come substantially into force with the proclamation of Parts 2 (Information Protection Principles) and 6 (public register provisions), and most of Part 5 (internal and external review).

WHAT IS PERSONAL INFORMATION?

The Act defines personal information as any information 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 also 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; and
- ▶ a number of exceptions relating to law enforcement investigations.

WHAT IS A PRIVACY CODE OF PRACTICE?

A code of practice under the *Privacy and Personal Information Protection Act 1998* is a statement about how an agency proposes to depart from or modify the operation of the Information Protection Principles or the public register provisions in the Act. Privacy codes of practice must be submitted to the Privacy Commissioner and approved by the Attorney General. Once made, an agency has a legal requirement to comply with their code.

A number of codes modifying the effects of the Information Protection Principles and public register provisions have been made in advance of the commencement of these provisions.

Provisions restricting disclosures of information to jurisdictions outside of NSW and empowering the Administrative Decisions Tribunal to award damages do not commence until 1 July 2001.

THE PRIVACY AND PERSONAL INFORMATION PROTECTION REGULATION 2000

The *Privacy and Personal Information Protection Regulation 2000* was gazetted on 30 June 2000 to commence on 1 July 2001. The Regulation:

- ▶ exempts public sector agencies staffed through a parent department from the requirement to prepare a separate privacy management plan;
- ▶ exempts the Torrens Title Register maintained under the *Real Property Act 1900* and associated indexes, the General Register of Deeds, and the Valuer General's Valuation Roll from the public register provisions in Part 6 of the Act; and
- ▶ exempts the Law Society and Bar

Association from all provisions of the Act. As statutory bodies they would otherwise have come under the Act's definition of public sector agencies.

PRIVACY MANAGEMENT PLANS

Part 3, Division 2 of the Act provides that agencies must prepare and implement a privacy management plan by 30 June 2000, providing a copy to the Privacy Commissioner as soon as practicable after it has been prepared. The Commissioner will monitor the standard and comprehensiveness of privacy management plans with a view to ensuring effective compliance with the Act.

Agencies will also be required to have copies of their privacy management plan available for public inspection or purchase as a policy document in accordance with section 15 of the *Freedom of Information Act 1989*.

Privacy NSW has played a major education and advice role in assisting agencies prepare their plans. At the end of the reporting period, Privacy NSW had received approximately 35 plans, with many more expected in early July 2000. In the 2000/2001 reporting year, it is intended that Privacy NSW will

develop guidelines for the assessment of privacy management plans.

PRIVACY CODES OF PRACTICE

In 1999 a privacy code of practice was prepared for the NSW Public Sector Workforce Profile to facilitate the collection of employee data about public sector employees by the Premier's Department for policy development and workforce planning. The code was recommended by the Privacy Commissioner and approved by the Attorney General in July 1999. Although the data collected for the Workforce Profile does not directly identify employees, it comes within the Act's definition of personal information which includes information or an opinion about an individual whose identity could reasonably be ascertained.

Privacy NSW assisted with the development of a number of other codes that were approved by the Attorney General during the year, including codes of practice for:

- ▶ the Legal Aid Commission;
- ▶ the NSW Police Service;
- ▶ law enforcement access to public registers;
- ▶ local government;
- ▶ the Bureau of Crime Statistics and Research;
- ▶ NSW Health; and
- ▶ the Office of the Director of Public Prosecutions.



Privacy NSW maintains and updates information on the Lawlink NSW website hosted by the NSW Attorney General's Department.

During the reporting year, Privacy NSW updated Internet information concerning various privacy matters,

including:

- ▶ details of the new legislation;
- ▶ calling number display and privacy;
- ▶ privacy and private mail, email, lockers, draws and computers at work;
- ▶ security fingerprint systems at work; and
- ▶ proposed privacy codes of practice.



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

KEY RESULT AREA:

Protection of Privacy

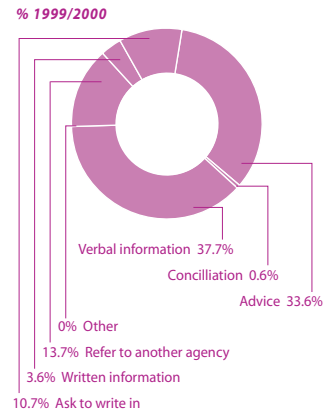
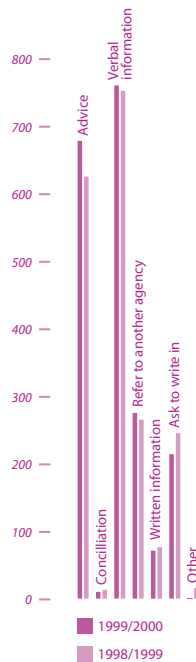
TELEPHONE QUERIES

Privacy NSW receives a number of telephone enquiries each year, which often take the form of requests for information or advice about privacy rights. In 1999/2000 Privacy NSW received 2021 phone queries, a slight increase on the number in previous years.

Since 1997/1998, Privacy NSW has increased the number of instances where information or advice has been provided over the phone by over 10 per cent (from 1222 to 1442). The number of referrals to other agencies has fallen by over 2 per cent.

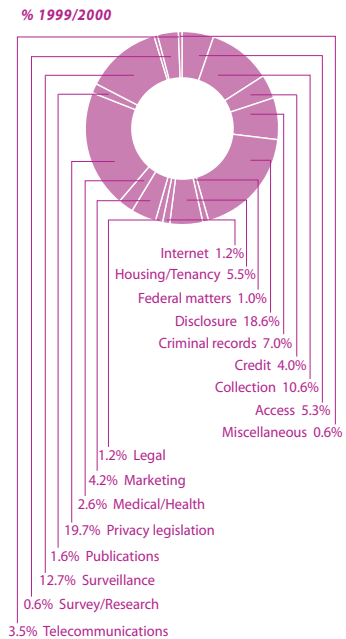
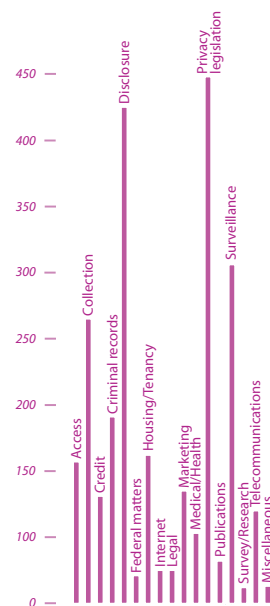
Of the 2021 calls received in 1999/2000, 922 were requests for advice or information and 1099 were complaints. Private employers and government agencies were the most common organisations complained about, a trend consistent with the previous reporting year. The most common subject of calls related to privacy legislation and the disclosure of personal information. Over 12 per cent of calls also related to surveillance issues.

Telephone queries action by Privacy NSW

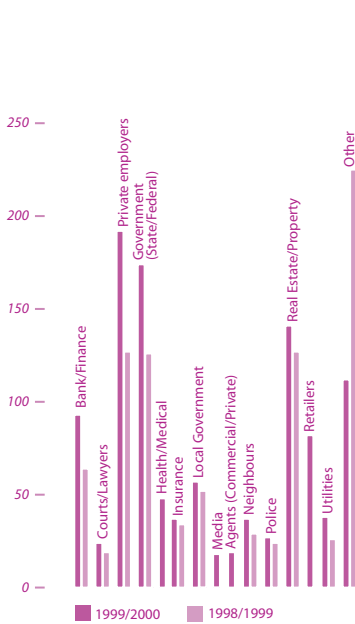


Total calls 1999/2000 – 2021
Total calls 1998/1999 – 2006

Subject of phone calls received 1999/2000

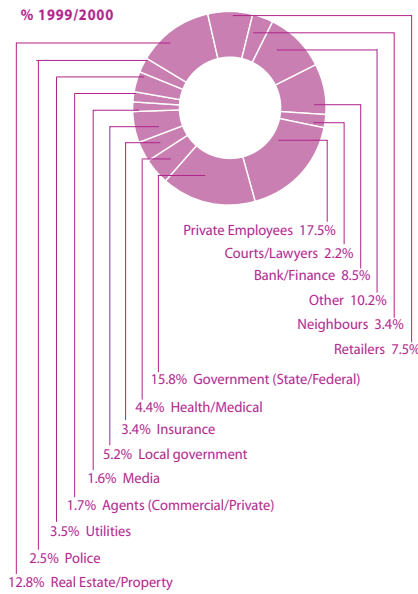
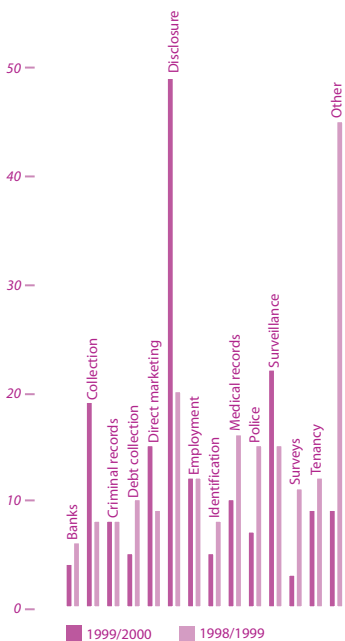


Complaints against



Total 1999/2000 – 2021
Total 1998/1999 – 2006

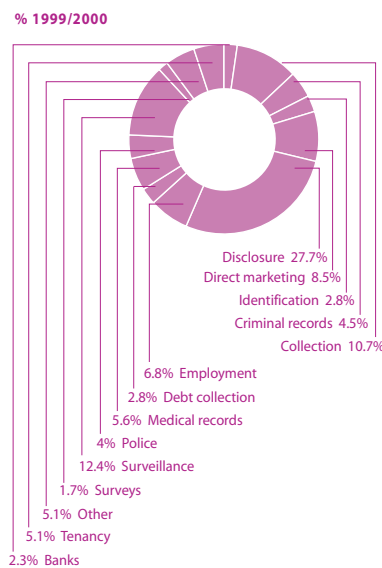
Complaint files subject category



COMPLAINTS

Under Part 4 of the Act, the Commissioner is responsible for accepting and considering complaints made by individuals who believe their privacy may have been breached. Complaints will range from neighbourhood disputes, to actions by private sector organisations and state government agencies. When investigating complaints, the Privacy Commissioner will apply Privacy NSW's Data Protection Principles and encourage organisations to adopt these principles in their activities.

Generally the Commissioner will not investigate a complaint unless it has been lodged in writing. In 1999/2000 the Commissioner closed files on 177 matters which had been investigated, and opened 227 complaint files. The most common subject of complaints in 1999/2000 concerned the disclosure of personal information. The number of complaints received about collection and disclosure issues has more than doubled since the 1997/1998 reporting year. The statistics also show an increasing number of complaints concerning surveillance issues, and a fall in the number of complaints about debt collection, policing and tenancies.



DATA PROTECTION PRINCIPLES IN BRIEF

The full text of the Data Protection Principles are available on the Privacy NSW website at www.lawlink.nsw.gov.au/pc.

PRINCIPLE 1

Manner and purpose of collection of personal information

Personal information should only be collected for a lawful purpose directly related to a function or activity of the collector.

PRINCIPLE 2

Solicitation of personal information from individual concerned

Personal information should normally be solicited directly from the individual concerned. At the time the information is collected, the individual should be advised why it is being collected, whether the provision of the information is compulsory and what other parties will have access to the information.

PRINCIPLE 3

Solicitation of personal information generally

Collectors of personal information should take reasonable steps to ensure that the personal information they collect is relevant, accurate, up-to-date and complete, and does not intrude to an unreasonable extent upon the personal affairs of the individual concerned.

PRINCIPLE 4

Storage and security of personal information

Organisations should ensure that personal information is stored appropriately and protected by appropriate security safeguards from

loss, unauthorised access, or misuse.

PRINCIPLE 5

Information relating to records kept by recordkeeper

Any person has a right to know whether an organisation holds personal information and, if so, its nature and purpose, the main purposes for which it will be used, the classes of persons about whom it is kept, the period for which the information is kept, the persons who are entitled to have access to it, and how to obtain access to it.

PRINCIPLE 6

Access to records containing personal information

A person has a right of access to their personal information held by an organisation, subject to exemptions under any law that provides for access by persons to documents.

PRINCIPLE 7

Alteration of records containing personal information

Organisations should make any necessary corrections, deletions and additions to personal information to ensure that it is accurate, up-to-date and complete. Organisations should, on request, add any reasonable statement a person wishes to see included in their record. Other recipients of the information should be informed about corrections.

PRINCIPLE 8

Recordkeeper to check accuracy etc. of personal information before use

Organisations should take reasonable

steps to ensure that personal information is relevant, accurate and up-to-date before use.

PRINCIPLE 9

Limits on use of personal information

Organisations should not use personal information for purposes other than for which it was collected except with the consent of the person concerned, to prevent a serious threat to a person's life or health, or as required or authorised by law.

PRINCIPLE 10

Limits on disclosure of personal information

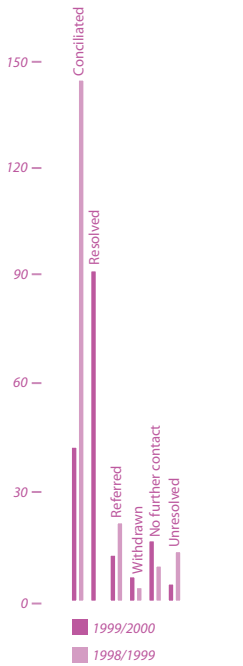
Organisations should not disclose personal information to other parties except with the consent of the person concerned, where the individual has been notified under principle 2 that such disclosures are usual practice, to prevent a serious threat to a person's life or health, or as required or authorised by law. The recipient of the information can only use it for the purpose for which it was disclosed.

PRINCIPLE 11

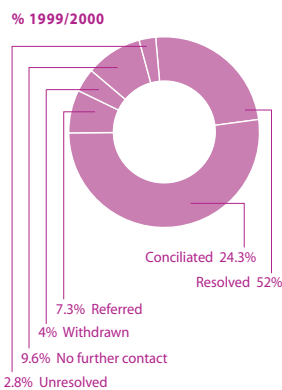
Sensitive personal information

Notwithstanding principles 9 and 10, information relating to ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, health or sexual life should not be disclosed by an organisation without the express consent, freely given, of the individual concerned. Criminal history information should only be used and disclosed in accordance with the guidelines endorsed by the NSW Privacy Commissioner.

Complaint outcome



Total 1999/2000 – 177
Total 1998/1999 – 195



Having received a complaint the Commissioner is required to undertake a preliminary assessment of the complaint. The Commissioner may decline to investigate a complaint if he or she considers it 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 the Commissioner decides to investigate a complaint he or she must endeavour to resolve the complaint by conciliation. The Commissioner seldom undertakes a formal conciliation process but attempts 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 prevent such breaches in the future.

More than 76 per cent of complaint investigations which were finalised in 1999/2000 were either conciliated or resolved. This is consistent with the previous year (in 1998/1999, conciliated and resolved complaints were grouped together in the category 'conciliated'). The number of unresolved complaints fell from over 7 per cent to less than 3 per cent in the same time period.

In May 2000, work began on a review of the Privacy NSW protocol for the handling of complaints. This protocol will be finalised in the next reporting year.

LEGISLATIVE CHANGES AND THE COMPLAINT PROCESS

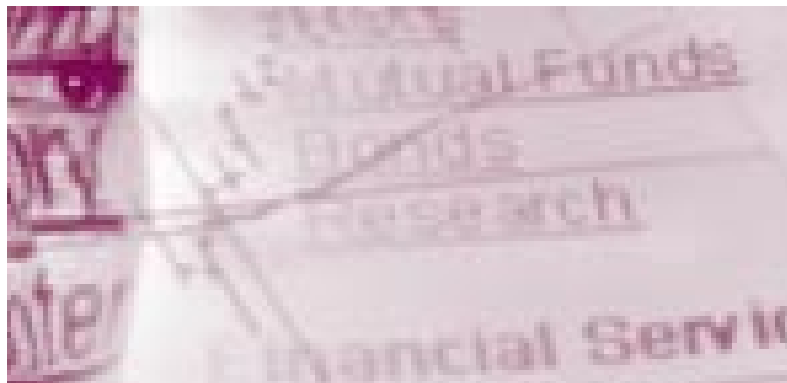
On 1 July 2000, most of the provisions in the Act relating to the Information Protection Principles (IPPs) and internal reviews will commence. The IPPs set out the privacy standards with which NSW public sector agencies will be expected to comply when dealing with personal information, subject to certain exemptions in the Act or privacy codes of practice. 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 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*.

Section 21 of the Act specifies that NSW public sector agencies must not contravene any IPP which applies to that agency. Any such contravention is conduct to which Part 5 applies. Under Part 5, a person aggrieved by the conduct of a NSW public sector agency will be entitled to an internal review of that conduct. The Act specifies at section 53 that such a review will be undertaken by the public sector agency concerned, and also sets out the obligations of an applicant when applying for an internal review.

Agencies will be required to deal with applications for internal review within 60 days and advise the applicant of the outcome of the review and any action proposed as a result of the review. If the agency fails to conduct an internal review within the specified timeframe or if the applicant is not satisfied with the outcome, an application can be made to the Administrative Decisions Tribunal for a further review. The Tribunal will have the power to make orders which are binding on the agency.

The NSW Privacy Commissioner may also have a role in the internal review process. A public sector agency that receives an application for an internal review will be required to notify the Privacy Commissioner of the application and keep the Privacy Commissioner informed of the progress and findings of the review. The Commissioner must also be notified of the action proposed to be taken by the agency in relation to the matter.

The Privacy Commissioner will also be entitled to make submissions to the agency in relation to the application, and may, at the request of the agency concerned, undertake the internal review on behalf of the



agency.

Where a complaint is made against an organisation which is not covered by the IPPs, the Privacy Commissioner will continue to apply the Data Protection Principles developed by the Privacy Committee in 1991, and will encourage organisations to adopt these principles in their activities. While the Data Protection Principles have a more general application than the IPPs, and are not subject to the exemptions which apply to the IPPs under the Act, they do not have any legal force.

COMPLAINT CASE STUDIES

Window view

Over the years the Privacy Committee and Privacy NSW have attempted with mixed success to resolve a series of complaints about

mailing practices. People are sensitive to the fact that mail addressed to them can be seen by other people and in some instances this may involve the inadvertent disclosure of information about them or their families. Organisations which send mail to selected groups should be sensitive to this and where possible avoid labelling or poorly fitting address windows which can disclose more than just a name and address.

In one case a shareholder complained about the way promotional printing on the envelopes used by firms to convey takeover information and offers revealed the identity of companies in which he held shares.

As the Corporations Law regulates the conduct of takeovers and use of personal details on shareholder



registers, the matter was referred in the first instance to the Australian Securities and Investments Commission (ASIC) for advice. ASIC did not wish to become involved in this issue pointing out that the conduct objected to did not depart from the provisions of the Act which allow companies to use a company share register to communicate with shareholders about affairs of the company. Two of the companies which had sent the correspondence were then approached. Relying on the fact that there was no legal breach, they did not consider that their conduct had been inappropriate.

In another case, the mother of an adult child who had previously taken part in a medical research survey, objected to a letter inviting the family to participate in a follow-up survey. The objection in this case

related to the placement of return address details which could be seen and conveyed the impression that the letter related to the mental health of a family member. The complaint was further complicated by the fact that a reminder letter was sent after the complainant had called to object.

The controller of the research project conceded that both of these aspects could have distressed family members and conveyed his apologies to the complainant. The complainant did not feel this was sufficient and was not entirely satisfied by the outcome.

It would be fair to say that both these cases point out the fact that some individuals, because of their particular circumstances, are likely to be more sensitive about the risks of disclosure than a mailer might reasonably expect. The risk of

causing offence cannot always be reasonably avoided. However some thought about what will appear on an envelope can prevent needless offence or distress.

It's criminal

A large national insurance company had included a question on its home contents insurance application form asking for the applicant to advise whether he or she had been the subject of criminal charges or convictions. Privacy NSW sought an explanation as to why the collection of the information about charges was necessary. It was also noted that any collection and use of criminal charge information would ignore the existence of the presumption of innocence, and that the collection of such information for the purpose of determining insurance risk was of questionable actuarial worth. The company advised that it would not enter this information onto its database and that it would not include any such questions on future applications forms.

Blood oath

A potential blood donor alleged that the Australian Red Cross Blood Service had breached his privacy by retaining the personal information he had provided in a donor declaration form. The donor alleged

that during a screening interview he was informed by a member of the Service's staff that his homosexuality placed him in a high risk category, and on that basis he was unable to donate blood. When asked why the information he had provided could not be returned to him the donor was informed that the information had been entered onto a database and that it could not be deleted. The Service told Privacy NSW that individuals who advise that they have engaged in homosexual activity since 1997 are permanently deferred, and are therefore ineligible to donate blood. The Service said that the reason it kept a permanent record of all applicants was based on experiences where deferred individuals had attempted donations on subsequent occasions. The Service also advised that despite its use of world best practice testing to screen donor blood, certain blood borne diseases are not detectable when blood is first collected. This 'window period' may span up to three weeks in some diseases and longer in the case of Human Immunodeficiency Virus (HIV). On this basis, the Service determined that it would maintain the categories of individuals who are permanently deferred.

Easy prey

A high profile television actor who had been convicted of a drink-driving offence and was subsequently sentenced to weekend detention in a Sydney Correctional Centre was the subject of a front page newspaper report. The photographs of the actor were taken while he and other inmates were at lunch during a working party outside the Correctional Centre. It appeared that the photographs had been taken from a concealed place with the use of a long-range lens camera. The article was highly critical of the allegedly generous conditions under which the actor and other inmates were detained. The article also contained detailed information about the activities of the inmates after they had been returned to the Correctional Centre.

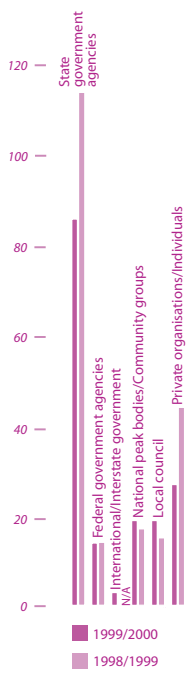
The newspaper was asked whether the inmates had been observed from a concealed place. At this stage, Privacy NSW pointed out that the use of covert surveillance of individuals results in unfairness, because it does not allow the subject of the surveillance freedom of movement or expression and it denies those individuals the opportunity to refuse to be watched. It was also pointed out that the publication of the story would be likely to have an adverse impact on

the acting career of the inmate and that the derogatory tone of the article might subject all the inmates who had been photographed to ostracism and vilification after their release. The newspaper was also asked to comment on how it obtained the information relating to the inmates' routines.

The newspaper refused to disclose the source of the information and it asserted that the means by which the inmates' photographs had been taken did not breach their privacy. It disputed that the actor's career might be impaired by the publication of the story and asserted that publication of the information was actually in the public interest.

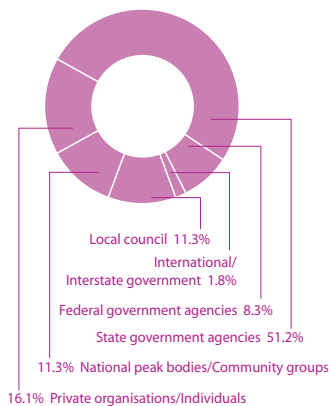
The then Chairman took the opportunity to express his views on the rights of detained persons to privacy. He pointed out that while the inmates were in a public space they were subject to detention and could not move from the view of the photographer, hence they were afforded less privacy than they would have enjoyed if they were in the Correctional Centre. The Chairman pointed out that Article 10 of the International Covenant on Civil and Political Rights requires that all persons 'deprived of their liberty' be treated with 'humanity and dignity'.

Source of requests for advice



Total 1999/2000 – 168
Total 1998/1999 – 204

% 1999/2000



ADVICE

Under Section 36 of the Act, one of the functions of the Privacy Commissioner is to provide advice on matters relating to the protection of personal information and the privacy of individuals. In the year 1999/2000 Privacy NSW closed 168 advice files, down from 204 in the previous reporting year.

The decline is partly explained by the fact that NSW government agencies are the primary source of requests for advice. From 1 July 2000, NSW government agencies will be required to comply with the Information Protection Principles and other associated provisions of the Act. In the reporting year, individual requests for advice from agencies fell as Privacy NSW prepared and conducted a series of education and training programs for agencies about their compliance requirements.

The number of requests from other sources has remained relatively stable, with the exception of a slight fall in requests from private organisations and individuals.

The Act had a particular impact on local councils owing to their close involvement with individuals in the community and the special disclosure provisions in the *Local*

Government Act 1993. This was reflected by an increase in the number of requests for advice received from local governments. The Act's public register provisions also had a significant impact on real estate agents and similar organisations who used councils as sources of property information.

The Acting Executive Member convened a Working Party on Local Government. The Working Party worked with local government representatives to come to terms with the distinctive ways in which the Act impacted on local councils. Major outcomes of this process were the *Model Privacy Management Plan for Local Government* and the *Privacy Code of Practice for Local Government*.

The privacy code of practice relaxed the requirements of the public register provisions by allowing people to inspect council records on council premises without requiring the person to provide a reason for accessing the register. However, restrictions on bulk copying of personal data were applied where the proposed use of information did not necessarily fit within the purpose for which the public register was created.

Advice issues have generally been

consistent between reporting years, except for a decline in requests for advice about law and legislation. This again may be explained by the training and education program conducted by Privacy NSW.

ADVICE CASE STUDIES

Video surveillance in retail, residential and recreational areas

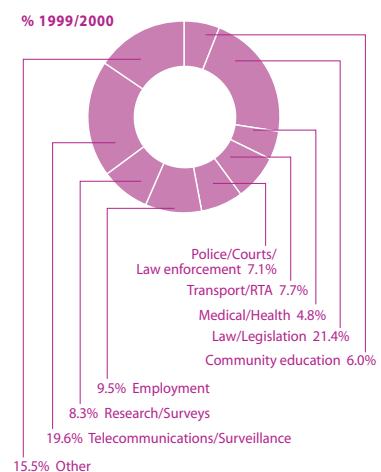
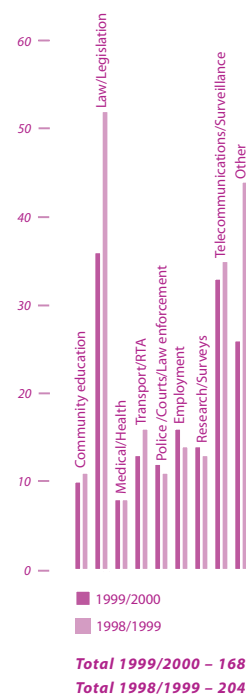
During the reporting period Privacy NSW continued to monitor the operation of street surveillance systems to ensure that they were consistent with guidelines agreed to by the NSW Police Service. The guidelines provide that such systems should be operated independently from the police, with appropriate police back-up. In August 1999 Privacy NSW became aware that one local council had set up street cameras which were being monitored from the local police station. As a result of advice provided by Privacy NSW, the operation of the system was suspended pending the establishment of a monitoring centre under the control of the council.

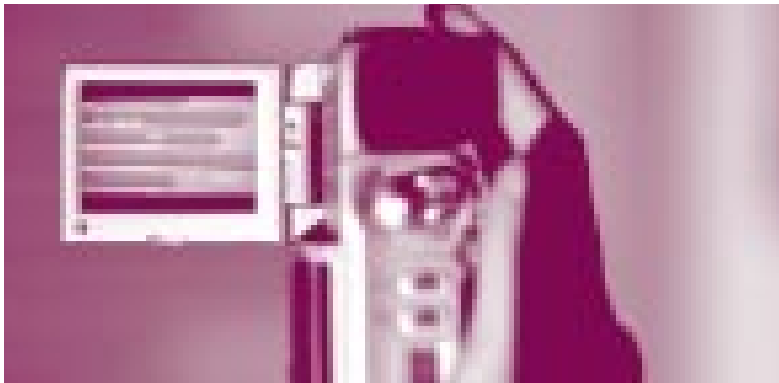
In May 2000 the resident's council of a tourist village sought advice from Privacy NSW concerning whether it

was reasonable to ask the management to turn off the video surveillance system in the village's recreation room while meetings were being held. Privacy NSW advised that such a request appeared to be reasonable, as the justification given for the camera was to deter vandalism and having it on during meetings, even without sound could be seen to inhibit the way council members expressed their views.

A report in the Sunday Telegraph of 5 September 1999, alleging that nightclub patrons had been secretly filmed in a bathroom for a music video clip, was also investigated by Privacy NSW. If these allegations were accurate, they would constitute a gross invasion of privacy as well as a possible breach of the *Workplace Video Surveillance Act 1998*. However, Privacy NSW was satisfied in this case that there had been an element of exaggeration in the news report. According to the producers of the video, the filming of club patrons had taken place in a powder room area which was physically separate from the toilet area, patrons had been warned by notice that they might be filmed, and were asked to sign a release form before entering the area being filmed.

Subject category





A Bill of Rights for NSW

In April 2000 the Privacy Commissioner made a submission to the NSW Legislative Council's Standing Committee on Law and Justice, supporting the proposal for a NSW Bill of Rights to enhance and protect the right to privacy.

The Commissioner noted that privacy was one of the rights recognised in international instruments such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, and argued that current statutory protection for privacy was limited in scope, applying largely to the systematic collection and use of personal information and some forms of covert surveillance. Even in those areas, current privacy protections operated unevenly with significant exemptions. The Commissioner argued that this was insufficient to

counter the historical neglect of individual privacy by common law. Legislative recognition of a right to privacy could do much to remedy this position, provided it was not easily amended and included an adequate means of enforcement by concerned individuals.

Genetic screening for newborn children

The Newborn Screening Program has been routinely screening all children born in NSW for a range of rare but treatable genetic conditions since 1976. The samples taken for testing are stored at the screening unit as 'Guthrie cards', dried samples of blood obtained from a pin prick to the infant's heel and stored on blotting paper. Similar screening takes place in other states and territories.

An article in the Sydney Morning Herald of 1 December 1999 drew

attention to the issue of access to the stored samples by police. The article reported that the Western Australian screening unit had recently decided to destroy its old samples after police had subpoenaed Guthrie cards for several members of one family.

Privacy NSW received a number of inquiries about the collection and retention of samples by the Newborn Screening Program at the same time. In response to these issues the Privacy Commissioner visited the facility where the cards are held and met with the Director of the Newborn Screening Program to clarify the collection and retention policies. Discussions covered:

- ▶ the reasons for testing and the procedures followed in screening, recording, storing and destroying cards;
- ▶ the brochure advising parents about the reasons for testing, the fact that tests are voluntary, and that individuals can apply to have the stored cards destroyed; and
- ▶ the policy for disclosing tests to police and law enforcement agencies.

Following these discussions the Privacy Commissioner made a number of recommendations on the advice contained in the brochure

and expressed an interest in following up the policy for law enforcement access. Currently, police are only given access to cards with the consent of relatives or next of kin to identify missing or deceased persons.

Data marketing

In June 1999 US database marketer, Acxiom Corporation, announced a joint venture with Publishing and Broadcasting Limited to establish Acxiom Australia to market client data to Australian businesses using the resources of both organisations. Publishing and Broadcasting Limited is a major force in Australian media and communications. Privacy concerns expressed to Acxiom Australia in response to the announcement reflected the scale of the database which the joint venture would create, and fears that it would promote the active profiling of customers by corporate clients. Controversy about the scheme intensified in late November with assertions that the company would collect financial data about consumers and federal government opposition claims that the Acxiom database would involve illegal use of electoral roll data.

On 30 November the Privacy Commissioner was interviewed on

ABCTV's 7.30 Report about the privacy implications of the scheme. He expressed concern that without adequate federal privacy legislation covering the private sector, consumers would have no remedies against the misuse of information collected on such a large scale.

Over the following six months Privacy NSW received several inquiries in response to this publicity. The Privacy Commissioner wrote to the CEO of Acxiom Australia who advised that the data collected would be used for direct marketing purposes and would not contain sensitive information such as bank records, credit history or Medicare numbers. Acxiom Australia was a member of the Australian Direct Marketing Association and would comply with its code of practice. Speaking at the *AdForum 2000* conference in March 2000, the CEO of Acxiom Australia urged marketers to act to ease consumers' privacy concerns before federal private sector privacy legislation was tabled.

The impact of this new player is likely to intensify existing direct marketing practices to which the Privacy Committee has drawn attention over the years. While it was difficult for Privacy NSW to take further action simply on this basis,

the controversy over Acxiom helped create a climate ready for the passage of federal privacy legislation covering the private sector.

RESEARCH

One of the functions of the Privacy Commissioner under section 36 of the Act is to conduct research, and collect and collate information, about any matter relating to the protection of personal information and the privacy of individuals. Issues subject to research are not static and are continually evolving. Files may remain open for a number of years to ensure that when the research is completed it is up to date and takes account of the most recent trends and issues.

During the year 1999/2001 Privacy NSW closed 10 research files. Some of these included:

- ▶ Smart Card Advisory Network;
- ▶ Health Information Association of NSW;
- ▶ Australian Police Ministers Council proposal for a National Paedophile Register; and
- ▶ NSW Freedom of Information Practitioners Network.

As part of this research function, it is essential that Privacy NSW maintains an awareness of current and emerging issues. One mechanism to

achieve this is through representation on relevant committees and advisory groups to enable Privacy NSW to provide comments when and where necessary. Examples of such representation by Privacy NSW during 1999/2000 included:

- ▶ Better Medical Management Systems Privacy Working Group;
- ▶ *Child Protection (Offenders Registration) Act 2000* Implementation Committee;
- ▶ NSW Ministerial Advisory Committee on Privacy and Health Information;
- ▶ NSW Health Privacy of Information Steering Committee; and
- ▶ Internet Service Providers Fraud Working Group.

FLASHBACK: HOW HAVE THE ISSUES CHANGED IN THE PAST TEN YEARS?

It is interesting to reflect on how privacy issues have evolved over time. Over the next few pages, an examination of matters reported on by the Privacy Committee in 1990 highlights how some issues have been effectively resolved, some still remain on the agenda, and some have resurfaced in another form, often through advances in technology.

Informed consent for medical testing

In 1990, the Privacy Committee reported that the National Centre for HIV Epidemiology and Clinical Research had screened 10,000 babies for AIDS antibodies without parental consent. The Privacy Committee noted that the valid and informed consent of the person to be tested (or legal guardian in the case of minors) for the collection of blood or other tissue is a fundamental requirement of ethical medical research. Without such consent there is a serious breach of physical privacy.

The issue of informed consent in relation to medical testing and care remains a primary issue in the privacy debate (for example, see the earlier reported advice case study concerning genetic screening for newborn children). One aspect concerns cases where a person is incapable of providing informed consent due to age or disability, and the procedure for obtaining consent from an adult or a nominated representative of that person. In the private sector there has been a lack of regulation in this area, despite a common law duty of disclosure and some requirements contained in health practitioner registration legislation (for example, the *Medical*

Practice Act 1992 and the *Dentists Act 1989*). There is also increased pressure on medical professionals to use and disclose patient medical information for purposes other than objective diagnosis and treatment which the patient has not consented to.

In the reporting year, the Privacy Commissioner examined the prospective use of electronic health records for improved diagnosis and treatment amongst citizens of NSW. Part of the agenda for such a system would be to ensure that patients could determine which providers in the health system (including private providers) could have access to all or some of their records held electronically and to provide protection against use of this information for purposes not consented to. In order for such a system to operate effectively, there would need to be systems of graded access to information (eg Dr X to get no information, Dr Y some and Dr Z all).

While clearly the issues involved in such a process are complex, the Privacy Commissioner is of the view that the medical profession will potentially need to be more directly involved with the issue of patient consent at all levels of relationships with their patients before any

electronic health record system could be contemplated. It is anticipated that Privacy NSW will continue its involvement in this issue into the future.

Report to the Chelmsford Royal Commission

The Chelmsford Royal Commission was established in the late 1980s to investigate the operation of the Chelmsford Private Hospital because of a number of deaths and serious injuries associated with the use of 'deep sleep' treatment between 1962 and 1979. There was concern that these deaths and injuries had not been dealt with adequately by existing legal and institutional mechanisms, such as peer review, the Health Department and the court system.

In 1990 the Privacy Committee made a submission to the Royal Commission into Chelmsford Private Hospital which highlighted:

- ▶ the need to protect disclosure of medical information concerning a patient's mental health to anyone outside of the primary care team unless consented to by the patient or otherwise authorised by law;
- ▶ access to records by the patient or a nominated representative;



- ▶ peer review of patient care; and
- ▶ informed and voluntary consent before undertaking experimental treatment.

The Chelmsford Private Hospital patients were extremely vulnerable to shortcomings in care due to their psychiatric conditions. This highlighted the need for medical professionals to ensure that a patient has the capacity to make informed decisions, and if not, to determine who has the authority to provide such consent.

In the intervening years, a medical practitioner's duty to disclose risks and obtain informed consent from the patient (or other person responsible) has been recognised by the High Court of Australia (see *Roger v Whitaker* [1992] 175 CLR 479 and *Chappel v Hart* [1998] 95 CLR 280). There has also been increased pressure for a legislative scheme to

protect health information in Australia, whether held by public or private organisations. This is especially important when considering the prospect of linked electronic health records.

Further, the *Private Hospital Regulation 1990* made provisions dealing with medical records held by private hospitals, specifically in relation to content, retention, right of access and confidentiality. These provisions were updated in 1996.

The Privacy Commissioner will continue to monitor and participate in issues concerning medical privacy and informed consent.

Powers of police to order medical examinations and to take body samples.

In May 1990 the *Crimes Legislation (Further Amendment) Bill 1990* was introduced into the NSW Parliament.



The Bill provided for an extension and clarification of the powers of police to order a medical examination of a person in custody or on bail, including the right to test for drugs and other illicit substances. The Privacy Committee was concerned that this could give police access to sensitive genetic and health information. The legislation did not proceed, but similar provisions were passed in 1995 amending section 353A of the *Crimes Act 1900* to allow for the collection of blood and saliva samples.

More recently, the *Crimes (Forensic Procedures) Act 2000* more fully codified the procedures for DNA testing, and also allowed for the taking of compulsory samples from suspects. The Act distinguishes

between two types of testing: intimate forensic procedure, including a buccal swab, where tissue is taken from the mouth cavity; or not-intimate forensic procedure. The legislation also identifies the conditions under which these procedures can be used – whether by consent only, by order of a senior police officer, or by order of a magistrate.

This legislation gives the police significant power to collect, store and use physical data information for the purposes of crime detection. The information obtained from the analysis of this forensic data will be stored on a national DNA database maintained by the Commonwealth and accessed by the States.

The use of genetic technology raises complex and disturbing privacy

issues. In essence, the legislation provides for the establishment of a database which would house the 'genetic' fingerprint of many Australians. While there would presumably be public support for this information to be used to solve serious crime there is always the possibility that the information so gained might be used inappropriately and for other purposes.

During the 1999/2000 reporting year, the Privacy Commissioner provided comment on the draft legislation to the Attorney General which highlighted a number of concerns.

While the Bill proposed penalties for matching material not lawfully collected, there was no mechanism to prevent such material from being used as evidence, creating the potential for exploitation of the process. The Bill also proposed to make it mandatory for all current detainees convicted of a serious indictable offence to be tested, allowing for material to be collected for general identification purposes rather than for the detection of a specific crime. The Privacy Commissioner suggested that police

should be required to justify a need for the sample, for example, by showing that the person was a likely suspect in an unsolved crime. Further, the creation of any DNA database would raise the potential for the information contained therein to be used by governments for other purposes (eg to create social profiles or to sell data).

While the federal government intended that similar legislation dealing with DNA testing would be mirrored by all states, this did not eventuate. As a result, the proposed NSW legislation did not establish a mechanism to prevent the inappropriate disclosure of information about DNA material collected in accordance with the defined process to other jurisdictions.

Compulsory DNA testing for criminal investigation purposes illustrates dramatically the potential for new technology to intrude upon an individual's very physical integrity, the ultimate privacy breach.

Electronic Vehicle Tracking

In 1989/1990, the NSW Police Service were promoting the Quicktrac system which involved owners installing radio controlled

transponders in their cars for the purposes of the police being able to track and recover vehicles in the event of theft. The Privacy Committee expressed concerns about Quicktrac being used by police for surveillance without the knowledge or consent of the owner. The Committee also published an issues paper on electronic vehicle tracking in 1990.

While this proposed scheme did not progress, there has been an increase in the use of various forms of surveillance to monitor and track the movement of vehicles by government and non-government agencies. The majority of this surveillance is used to determine the use and whereabouts of vehicles.

Examples include:

- ▶ Safe-T-Cam, operated by the Roads and Traffic Authority (RTA) to monitor heavy vehicle movements and record keeping requirements;
- ▶ tracking devices installed on the outside of vehicles by police and private inquiry agents without consent to monitor vehicle movement;
- ▶ fixed speed and red light cameras, first introduced in 1987/88; and
- ▶ traffic control cameras to assess

major traffic blockages and improve traffic flows.

The NSW Government has also proposed that vehicles travelling on tollways be billed through the electronic recording of their entry to and exit from the tollways. While there may be broad community support for many of these initiatives, they remain generally unregulated. In the absence of such regulation, any information obtained through the use of such surveillance devices may be collected, used and/or disclosed for purposes other than the stated primary purpose. The transfer of such information between different government agencies, particularly between the RTA and the NSW Police Service, remains a source of concern for the Privacy Commissioner.

In this light it is pleasing to see that the Attorney General has asked the NSW Law Reform Commission to report on all aspects of surveillance activity in NSW. It is hoped that the report may lead to effective regulation of these activities.



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

During the reporting period a major priority for Privacy NSW was to present information to public sector agencies about the new legislative requirements. As reported in 1998/99, Privacy NSW encouraged agencies to appoint privacy contact officers to facilitate communications with the Privacy Commissioner and through whom advice and information about the Act could be disseminated. In August 1999, Privacy NSW hosted a meeting of privacy contact officers to explain the various requirements of the new legislation.

Privacy NSW engaged a consultant to develop a training package to outline the responsibilities of public sector agency staff responsible for putting the Act into effect. The training program emphasised the importance of the preparation of privacy management plans and the need to consider whether the agency might need to apply for a privacy code of practice. The course was piloted in October 1999, and was subsequently delivered jointly by staff of the Training Unit of the Attorney General's Department and Privacy NSW from November 1999 to March 2000.

The Privacy Commissioner and staff of Privacy NSW also gave presentations to a number of gatherings within the NSW public sector. Local Government was identified as a special target audience given requirements of the *Local Government Act 1993* for access

to council documents and in light of the fact that local government holds large amounts of personal information about individuals. Privacy NSW initiated discussions with the Local Government and Shires Associations on a training package, specially tailored for local councils to be implemented in the next reporting period. Staff also spoke to meetings of council officers in various regions.

Presentations by Privacy NSW included:

- ▶ Privacy Contact Officer Network;
- ▶ Government Lawyers Forum;
- ▶ Investigative Agencies Briefing;
- ▶ Department for Women;
- ▶ Department of Education and Training;
- ▶ Department of Land and Water Conservation;
- ▶ FOI Practitioners Network;
- ▶ the NSW Police Service;
- ▶ Wollongong City Council Network; and
- ▶ Government Legal Department Heads.

An essential support to the training program included the publication of a series of guidelines, to give concise summaries of the Act. *The Privacy and Personal Information Protection Act: A Plain English Guide* (1999) provided a general overview. Other publications included:

- ▶ A Guide to Making Privacy Codes of Practice (1999);
- ▶ A Guide to Making Privacy Management Plans (1999);
- ▶ A Guide to Internal Reviews (2000);
- ▶ A Guide to Public Registers (2000); and
- ▶ A Guide to the Information Protection Principles (2000).

These guidelines described how the Privacy Commissioner intended to view each of the main topic areas of compliance, and recommended a standard approach by agencies. Copies of the publications were provided to each public sector agency and to officers attending the training courses.

Staff of Privacy NSW also participated in an intensive mediation training course conducted for the Anti-Discrimination Board by the Australian Commercial Disputes Centre to prepare for the more conciliation based approach to complaints mandated in the new legislation.

FEEDBACK ON PRIVACY TRAINING CONDUCTED BY PRIVACY NSW

'Helpful and informative'

'I had a very limited idea of Privacy and how it would effect my agency. After the training I now know what it is all about'

'Great Course. Would like to see further courses on this matter'

'Most informative and thought provoking'

'Good course to attend'



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



KEY RESULT AREA:

Consultation and Partnerships

In the reporting period Privacy NSW was involved in consultation with various privacy agencies, public sector agencies and key stakeholder groups.

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. In March 2000, the PANZA meeting was hosted by the federal Privacy Commissioner in Sydney and attended by representatives of Privacy NSW.

Jurisdiction reports were provided by the New Zealand Privacy Commissioner, the Northern Territory Attorney General's Department, the South Australian Privacy Committee, Multimedia Victoria, the Queensland Department of Information and Innovation Economy, the West Australian Information Commissioner and the Hong Kong Privacy Commissioner (a long-standing guest member). The NSW Privacy Commissioner took the opportunity to provide privacy

agencies with an overview of the Act and the operations of Privacy NSW.

The federal Privacy Commissioner, Mr Malcom Crompton, announced that from 1 July 2000 the connection between that office and the Human Rights and Equal Opportunity Commission had been severed by the passage of the *Privacy Amendment (Office of the Privacy Commissioner) Act 2000* (Cth) which established the Commission as a separate statutory body. The Commissioner also outlined the *Privacy Amendment (Private Sector) Bill 2000* which proposed private sector privacy legislation.

The New Zealand Privacy Commissioner Mr Bruce Slane presented a paper on the forensic use of DNA which discussed the issue of taking samples from suspects and the creation of DNA profile databanks. Mr Slane also discussed matters relating to cross-border data matching, sports drug testing and health information.

Mr Tony Lam from the Office of the Hong Kong Privacy Commissioner for Personal Data presented a Consultation Paper on Civil Liability for Invasions of Privacy. The Paper recommended the creation of two torts for invasion of privacy by intrusion upon another's seclusion or solitude and invasion of privacy

based on public disclosure of private facts. In the proposed model both torts would be actionable without any requirement for proof of damage. Mr Lam also presented papers on the regulation of media intrusion and compliance checks of Hong Kong based websites.

CONSULTATION ON THE PRIVACY AMENDMENT (PRIVATE SECTOR) BILL 2000

In September the federal Attorney General's Department held public consultation on an Information Paper concerning the *Privacy Amendment (Private Sector) Bill 2000*. The consultation took place in response to the federal government's undertaking in December 1998 that it would develop 'light touch' private sector legislation.

The Bill proposed the implementation of the National Principles for the Fair Handling of Personal Information (NPPs), which regulate the collection, use, storage, transfer and disclosure of personal information. The NPPs also grant individuals access to and correction of their personal information. Private organisations may choose to be bound by the NPPs or may apply to have a privacy code of practice approved by the Privacy Commissioner. There are exemptions

for research, media organisations, employee records, government business enterprises and small business.

Privacy NSW prepared a submission on the Information Paper and suggested that the proposal to extend the NPPs to the private sector or to allow organisations to create their own code schemes would not provide adequate privacy protection. Privacy NSW argued that:

- ▶ allowing organisations to prepare their own privacy codes for approval by the Privacy Commissioner would result in a patchwork of privacy schemes which would create confusion and discourage individuals from making privacy complaints;
- ▶ exempting employee records from the ambit of the legislation would adversely affect the rights of employees to access and correct unfair information on personnel files, and employees should be confident that their personal information would be held securely;
- ▶ exempting information collected prior to the full commencement of the legislation fails to recognise modern methods of information processing which often involve the collection of information at different times in discrete fields in relational or object oriented databases. By attempting to

maintain an artificial distinction between information collected or created before or after commencement would most likely impose extra costs on business by mandating record systems which are capable of recording and distinguishing between the date on which information was created, added to, combined or modified; and

- ▶ providing a blanket media exemption fails to recognise community concerns about media privacy invasions. The exemption should be more precisely defined to prohibit the reporting of matters which exploited privacy breaches by others.

In December 1999 the federal Attorney General's Office sought further comment on the key provisions of the proposed legislation. The NSW Privacy Commissioner's response pointed out that a fully informed appraisal of the proposed legislation was not possible as the federal government had not provided the full text of the Bill.

This advice notwithstanding, the Commissioner made the following comments on some of the key provisions:

- ▶ the provision exempting bodies corporate from sharing information with related organisations failed to take

account of existing obligations of secrecy and/or confidentiality placed upon organisations, and assumed that functions are related on the basis of common ownership;

- ▶ the media exemption was broad enough to permit any organisation to disclose personal information so long as the information was made available to the public at large;
- ▶ the definition of small business placed the onus on individuals to know whether the business would be subject to the legislation before deciding whether to allow a business to collect their personal information; and
- ▶ greater emphasis should be given to the issue of express consent in order to prevent organisations relying on implied or imputed consent.

In June 2000 Privacy NSW gave evidence to the House of Representatives Standing Committee on Legal and Constitutional Affairs concerning the National Privacy Principles. The matters raised in evidence placed particular emphasis on the following:

- ▶ the possibility that organisations might bury or sidetrack a complaint;
- ▶ the difficulty in ascertaining whether individuals had in fact

provided informed consent to an organisation's dealings with their personal information;

- ▶ information held by employers might relate to employee medical history, family information, results of psychometric testing and biometric data and should therefore be afforded the same protection as personal information collected by organisations subject to the principles; and
- ▶ the creation of too many exemptions may be likely to cause individuals confusion and discourage compliance on the part of subject organisations.

PRIVACY ADVISORY COMMITTEE

Part 7 of the 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; and
- c) to advise the Minister on matters referred to it by the Minister.

Meetings of the Committee are chaired by the Privacy Commissioner. The Committee consists of up to six members, two from the Parliament of NSW (representing both the government and the opposition) and others from



people with a special knowledge of or interest in privacy matters. On 1 July 1999 the members of the Privacy Advisory Committee were:

- ▶ Professor Joan Cooper, University of Wollongong;
- ▶ Mr William Grant, Deputy Director General, NSW Attorney General's Department;
- ▶ Ms Gail Gregory, NSW Labor Council;
- ▶ Mr Mark Richardson, Law Society of NSW;
- ▶ Hon. John Hatzistergos, MLC (representing the Government); and
- ▶ Hon. Jim Samios, MLC (representing the Opposition).

Ms Gail Gregory, resigned from the Committee in July 1999 and Mr Mark Richardson in December 1999. On 16 February 2000 the Attorney General appointed Ms Naomi Steer, NSW Labor Council, and Mr Shaugn Morgan, Law Society of NSW, to the Committee.

The Committee met on 8 September and 22 December 1999. The meeting

of 8 September 1999 considered the Privacy NSW publication *A Plain English Guide to the Privacy and Personal Information Protection Act*. The meeting also received reports from Privacy NSW staff on current work.

The Meeting of 22 December 1999 received a report concerning the work done by Privacy NSW on implementing the new privacy legislation, and on the privacy management plan for the Attorney General's Department. The Committee also considered reports on the retention of photographs of drivers licence holders by the Roads and Traffic Authority and recent matters involving the protection of genetic information.

There were no independent references from the Attorney General to the Committee.



To ensure that the administrative framework of Privacy NSW supports all officers in their work

KEY RESULT AREA:

Administration

Privacy NSW participated in a number of administrative initiatives of the Attorney General's Department throughout the reporting year, either directly as an administrative arm of the Department or by providing privacy related comments. Some of these included:

- ▶ the draft Workplace Relationships Guidelines for staff;
- ▶ an occupational health and safety survey to increase staff awareness of occupational health and safety management;
- ▶ the Y2K desktop compliance assessment to identify potential problems with databases and files, and appropriate rectification strategies;
- ▶ a data improvement strategy and data audit;
- ▶ the 1999-2002 information technology strategic plan;
- ▶ a flexible working hours discussion paper;
- ▶ a records management survey under the *State Records Act 1998*; and
- ▶ a review of the code of conduct.

Privacy NSW internal administrative initiatives included:

- ▶ the establishment of new accounts procedures for receipts and revenue;
- ▶ a review of procedures for resource and information sharing with the Anti-Discrimination Board;



- ▶ the completion of an information technology review, which involved the upgrading of personal computers for Privacy NSW staff; and
- ▶ a review concerning the impact of the GST on Privacy NSW, which included recommendations about receipts and invoices, registering for an ABN and liaising with stakeholders and service providers to update processes for compliance.

An analysis of accommodation requirements was also completed. The different locations of Privacy NSW and the Anti-Discrimination Board were identified as an issue that impeded effective work processes, given that the Privacy Commissioner also holds the role of President of the Board. A decision was made to move into the same premises as the Board when their lease expired later in the reporting

year. Privacy NSW moved to the new Elizabeth Street premises with the Board on 2 March 2000.

STAFFING

The staffing structure of Privacy NSW was directly transferred from the former Privacy Committee and consisted of the following positions:

- ▶ Privacy Commissioner;
- ▶ Executive Member, Special Grade;
- ▶ Director, Research and Policy, Clerk 11/12;
- ▶ Investigations Officer, Clerk 7/8;
- ▶ Research Officer, Clerk 5/6 (2 positions); and
- ▶ Executive Assistant, Clerk 3/4.

However, during the reporting year this staff structure was reviewed to better meet the requirements of the new legislation. A new structure has been approved and will be implemented in the next reporting period.

FINANCIAL STATEMENTS

In 1999/2000, Privacy NSW was allocated a total budget of \$570,000, of which \$504,000 (net) was spent.

| | ACTUAL \$'000 | BUDGET \$'000 |
|--|------------------|------------------|
| REVENUE | | |
| Court fees | 0 | 0 |
| Other user charges | 4 | 0 |
| Other revenue | 47 | 0 |
| TOTAL REVENUE | 51 | 0 |
| EXPENSES | | |
| Employee Related Payments | | |
| Salaries and wages - permanents | 203 | 293 |
| Salaries and wages - temporary | 39 | 72 |
| Salary recoveries | 0 | 0 |
| Allowances | 0 | 0 |
| Overtime | 0 | 0 |
| Leave entitlements | 16 | 5 |
| Worker's compensation | 3 | 2 |
| Payroll tax | 17 | 25 |
| Fringe benefits tax | 0 | 0 |
| Superannuation | 0 | 0 |
| Redundancy | 0 | 0 |
| Total employee related payments (excluding crown liabilities) | 277 | 397 |
| Other operating expenses | | |
| Advertising and publicity | 2 | 0 |
| Audit external | 0 | 0 |
| Bank charges | 0 | 0 |
| Consultancies | 9 | 0 |
| Contractors | 0 | 0 |
| Electricity and gas | 7 | 4 |
| Fees | 52 | 23 |
| Freight and cartage | 0 | 0 |
| General expenses | 6 | 0 |
| Insurance | 1 | 0 |
| Interest paid | 0 | 0 |

| | ACTUAL \$'000 | BUDGET \$'000 |
|---------------------------------------|------------------|------------------|
| Other operating expenses con't | | |
| Interpreters/translations | 0 | 0 |
| Motor vehicles | 0 | 0 |
| Out-of-pocket expenses | 0 | 0 |
| Postal | 2 | 0 |
| Printing | 20 | 3 |
| Publications | 4 | 5 |
| Rates and outgoings | 6 | 3 |
| Removal costs | 0 | 0 |
| Rent | 98 | 84 |
| Staff expenses | 6 | 3 |
| Stores and stationery | 36 | 3 |
| Telephone | 11 | 24 |
| Travel | 0 | 1 |
| Transcription services | 3 | 0 |
| Witness expenses | 0 | 0 |
| Other expenses | 0 | 0 |
| Total other operating expenses | 264 | 154 |
| Total maintenance | 1 | 1 |
| Grants and subsidies | 0 | 0 |
| Other services - not protected | 0 | 0 |
| TOTAL EXPENDITURE | 542 | 552 |
| Less: Revenue | 51 | 0 |
| NET COST OF SERVICES | 491 | 552 |
| Plus: Depreciation | 13 | 18 |
| NET POSITION | 504 | 570 |

PUBLICATIONS AVAILABLE FROM PRIVACY NSW

| | |
|--|--------|
| Privacy and Personal Information Protection Act: A Plain English Guide | \$5.00 |
| A Guide to Making Privacy Codes of Practice (1999) | \$5.00 |
| A Guide to Making Privacy Management Plans (1999) | \$5.00 |
| A Guide to Internal Reviews (2000) | \$5.00 |
| A Guide to Public Registers (2000) | \$5.00 |
| A Guide to the Information Protection Principles (2000) | \$7.25 |
| Privacy NSW Annual Report 1998/1999 | free |

*Note that after 1 July 2000, these publications will be subject to a 10% GST.
Some publications of the former Privacy Committee are also available.
Please contact Privacy NSW for details.*

Privacy NSW

Office of the Privacy Commissioner
PO Box A2122, Sydney South 1235
Level 17, 201 Elizabeth Street,
Sydney 2000

T (02) 9268 5588

F (02) 9268 5501

www.lawlink.nsw.gov.au/pc

Hours of business are 9am to 5pm
Monday to Friday